NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WIRELESS SENSOR BUOYS FOR PERIMETER SECURITY OF MILITARY VESSELS AND SEABASES

by

Stephen D. Kent

December 2015

Thesis Advisor: Gurminder Singh
Co-Advisor: John Gibson

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2015	Master's Thesis

4. TITLE AND SUBTITLE
WIRELESS SENSOR BUOYS FOR PERIMETER SECURITY OF MILITARY VESSELS AND SEABASES

5. FUNDING NUMBERS

6. AUTHOR(S) Stephen D. Kent

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Naval vessels at anchor and seabases are vulnerable to attack by small surface crafts. The past two decades have demonstrated that attacks of this type are indeed possible, and that current security measures may not be sufficient to mitigate such a threat. As technology matures, it should be implemented into providing security for these valuable naval assets. An example of technology to be incorporated is wireless sensor networks. These wireless sensor networks have been utilized in recent conflicts, in the form of unattended ground sensors, with a high degree of success. By incorporating these ground sensors in an open ocean environment, attacks by small surface crafts toward naval vessels and seabases may be precluded.

The innovation of attaching wireless sensor nodes to buoys and positioning them around naval vessels to provide the necessary standoff against attack was investigated. Wireless sensor buoys were created using commercial-off-the-shelf products and existing prototype wireless sensor nodes. The tests that were conducted during this thesis determined that the current sensor nodes are suitable, and could be implemented in creating an ad hoc network on an open ocean environment. Future work to include the addition of alternate sensor modalities and longer ranging networks should be investigated.

14. SUBJECT TERMS
Ad-Hoc Network, Adaptable sensor system, Expeditionary Force 21, Light Detection And Ranging, Passive Infrared, Scheduler and Asynchronous/Synchronous, seabase, Shared Information Space, Unattended Ground Sensors, Wireless Sensor Buoys, Wireless Sensor Network

15. NUMBER OF PAGES
131

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

WIRELESS SENSOR BUOYS FOR PERIMETER SECURITY OF MILITARY VESSELS AND SEABASES

Stephen D. Kent
Captain, United States Marine Corps
B.S., Embry-Riddle Aeronautical University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2015

Approved by: Gurminder Singh
Thesis Advisor

John Gibson
Co-Advisor

Peter Denning
Chair, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Naval vessels at anchor and seabases are vulnerable to attack by small surface crafts. The past two decades have demonstrated that attacks of this type are indeed possible, and that current security measures may not be sufficient to mitigate such a threat. As technology matures, it should be implemented into providing security for these valuable naval assets. An example of technology to be incorporated is wireless sensor networks. These wireless sensor networks have been utilized in recent conflicts, in the form of unattended ground sensors, with a high degree of success. By incorporating these ground sensors in an open ocean environment, attacks by small surface crafts toward naval vessels and seabases may be precluded.

The innovation of attaching wireless sensor nodes to buoys and positioning them around naval vessels to provide the necessary standoff against attack was investigated. Wireless sensor buoys were created using commercial-off-the-shelf products and existing prototype wireless sensor nodes. The tests that were conducted during this thesis determined that the current sensor nodes are suitable, and could be implemented in creating an ad hoc network on an open ocean environment. Future work to include the addition of alternate sensor modalities and longer ranging networks should be investigated.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADAPT	Adaptable sensor system
AP	Access Point
ARA	Applied Research Associates, Inc.
AT/FP	Antiterrorism Force Protection
COTS	Commercial Off-the-Shelf
DARPA	Defense Advanced Research Projects Agency
DOD	Department of Defense
DODINST	Department Of Defense Instruction
EF-21	Expeditionary Force 21
GPS	Global Positioning System
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
ISR	Intelligence, Surveillance, and Reconnaissance
LCS	Littoral Combat Ship
LiDAR	Light Detection And Ranging
LTE	Long Term Evolution
MAC	Medium Access Control
MAGTF	Marine Air Ground Task Force
MANET	Mobile Ad hoc Network
MSAT	Mobile Situational Awareness Tool
NTTP	Navy Tactics, Techniques, and Procedures
PIR	Passive Infrared
SAS	Scheduler and Asynchronous/Synchronous
SIS	Shared Information Space
SSDF	Ship's Self-Defense Force
UAV	Unmanned Aerial Vehicle
UGS	Unattended Ground Sensor
USB	Universal Serial Bus
USMC	United States Marine Corps
USV	Unmanned Surface Vessels

UUV	Unmanned Underwater Vehicles
VTUAV	Vertical Take-off and Landing Tactical Unmanned Aerial Vehicle
WSB	Wireless Sensor Buoy
WSN	Wireless Sensor Network

ACKNOWLEDGMENTS

First and most importantly, I would like to thank my wife, Pascal, for her support, guidance, and inspiration. Her love, care, and devotion to our marriage is beyond imaginable, and I am very proud and fortunate to be her husband.

I would also like to thank JJ, Chris, and Tarry from the Oceanography Department at the Naval Postgraduate School; their assistance made this thesis possible. It was an absolute pleasure to work with them.

Thanks to Ms. Shirley who assisted on her days off to help with purchasing the materials required, to Peter for helping to transport the materials, to my thesis advisors, Gurminder and John, for giving me advice and helping to scope my thesis, and Billy for answering my technical questions regarding the ADAPT nodes.

I thank Kevin Killeen for giving me the idea to explore this topic, and Simon Sanchez and Alex Rawls for the help while conducting the testing.

Lastly, I want to thank my family and friends for their support and encouragement during this project.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Security is an essential aspect of conducting military operations. An adversary may attempt to attack a high valued target to achieve a tactical, operational, strategic, and/or political goal. Such an attack may occur from any direction, so complete coverage around the high valued asset is necessary. A perimeter security provides a degree of standoff to allow space and time in order to defend the asset against a threat, it also allows for the necessary all-around coverage of protection. Perimeter security is not a new concept; it has been used for hundreds of years in castles and forts to mitigate the effects of an attacking force and to keep the occupants within safe. Perimeter security is still in use today as modern homes often incorporate a fence to keep intruders off of one's personal property; it also further extends to prisons and to borders. As modern technology continues to develop, so do methods to protect property and assets. Some critical facilities such as military bases, nuclear power plants, and borders have begun to investigate emplacing concealed unattended ground sensors (UGSs) to further enhance the security of their perimeter [1]. These UGSs may include various detection modalities such as seismic sensors, infrared sensors, or cameras to alert the response force that an intrusion has occurred.

Naval vessels have adapted to defending against the attacking enemy by implementing modern weaponry and sensing equipment; however, as the current enemy has resorted to insurgent means where the threat is often indistinguishable, they conduct terrorist style attacks to achieve their goals. In the past two decades examples have demonstrated that naval vessels are vulnerable to such attacks and raising concern. Most naval vessels use mobility to reduce the likelihood of a planned attack; however, the USMC's intent to conduct seabasing poses a greater risk as seabases are less mobile than ships merely at anchor. All naval vessels incorporate an antiterrorism force protection (AT/FP) plan to mitigate an attack or preclude it from achieving its intent. Terrorist attacks, imminent in modern times, may be mitigated through enhanced force protection intelligence, training, readiness, and technology.

The Navy conducts a thorough protection of its ships, yet the likelihood of a breach in security is still possible, and while the security is reasonable, it can be enhanced by using technology in the form of a wireless sensor network (WSN) to act as a perimeter defense. A type of WSN that has been applied to military application is UGSs. UGSs are not a new concept; they have been in use for decades with reports of success. In recent times, these devices have become highly effective in the counter-insurgency fight [2]. Their effectiveness has also improved as technology matures and they incorporate advances modalities, improved wireless technology, and more reliable hardware and software.

Other technology exists to deter or prevent enemy attacks against naval vessels. Sonar has existed since the early twentieth century to detect underwater threats and was critical in defeating the Axis submarines during the Second World War. Sonar has even been employed on buoys to facilitate the combined use of assets to defeat the enemy [3]. In addition to sonar, modern technology allows for unmanned vehicles to counter threats at sea. Possessing advanced optics and detection equipment, and able to operate for extended times, unmanned vehicles can be deployed in the air, on the surface, and the subsurface to improve the Navy's force protection significantly.

In addition to sonar and unmanned vehicles, WSNs is a technology that can be incorporated into the protection of valuable assets. As this relatively new technology continues to develop, implementing it in the military domain is costly and complex. To mitigate the cost, the military may make use of commercial off-the-shelf (COTS) products integrating their capabilities with emerging sensor technologies. UGSs have many applications and can synchronize with other devices, when interconnected by an ad hoc network, to enhance their capability. One such application is to send the data to a handheld device and graphically depict the battlefield [4].

The United States Marine Corps (USMC) intends to broaden its operations in the littoral regions with the use of seabasing to improve logistical response over a larger area [5]. Although current security measures exist to protect naval vessels and seabases, a current shortfall exists to detect and prevent attacks from small surface attack crafts. In addition to the threat of small surface crafts, budget cuts imposed on the Navy limit crew

members to perform their required duties and the ever-increasing collateral duty responsibilities; this has a direct impact on the force protection of the vessels as sailors experience greater levels of fatigue. A system that could assist in mitigating the small surface craft threat and assist the sailors in their force protection responsibilities is the concept of a wireless network providing a secure perimeter, essentially a virtual wall.

B. OBJECTIVE

Current naval vessels and seabases are limited in their capabilities to defend against an attack from a small surface attack craft. The purpose of this thesis is to provide a wireless networking to be leveraged as part of a larger solution to this limitation by using modern technology wireless sensor nodes with inherent networking capability mounted on buoys to provide a secure perimeter to these platforms afloat. These wireless sensor buoys (WSBs) would detect any breach by a small surface craft into the security area surrounding the vessel being protected and notify the base station monitored by the watch crew located on the vessel of the impending threat. The proposed networking solution must be tested thoroughly to validate the viability of such a utilization of the devices. The scope of this thesis will address the design and performance of a wireless sensor network utilizing emerging Defense Advanced Research Projects Agency (DARPA) sensor nodes in order to validate the proposed capability.

The sensor "nodes" may be equipped with multiple modalities to detect an intrusion; however, a "node" that contains passive infrared (PIR) was readily available and selected for use during this thesis. These devices include a global positioning system (GPS) receiver to determine their location and an onboard power source for extended operations. They also utilize COTS technology and conduct all distributed detection processing to allow for a scalable network. Lightweight and small in size, they may be easily stored on naval vessels. Integrated communications systems enable formation of a network between the sensor nodes and to a remote monitoring node. The software applications onboard control the device location reportings, PIR sensors, detection data, and threat tracking data [4].

The prototype spar-buoys developed to host the existing sensor nodes, using low-cost COTS materials, proved effective in the sea environment. Testing was conducted in an incremental manner to confirm capability, functionality, and feasibility. The WSBs have several advantages that include relatively low cost due to the use of COTS components. In addition, the size and weight of the buoys allow for ease of storage and employment.

Testing the system identified numerous weaknesses of the WSBs. The PIR detections were not forwarded to the base station while operating on the ocean surface, potentially due to the high frequency of detections produced as a result of the turbulent water surface. While lightweight and small, the WSBs were difficult to emplace. Records were not always maintained and updated by the developmental SIS database. Further refinement of the sensor network topology as well as incorporation of more capable sensor modalities was suggested.

C. THESIS ORGANIZATION

The remainder of this thesis explores in detail the current shortfall in security of naval vessels and seabases and presents WSBs as a possible solution. Chapter II provides insight into the problem domain by describing the operational concept of perimeter security and historical events that suggest small surface attack craft are a threat that is difficult to prevent. Current tactics, techniques, and procedures are assessed and potential gaps in security are identified. The use of UGSs for military applications is discussed and how similar devices such as sonar and unmanned vehicles may help to mitigate adversary threats. Chapter III analyzes the overall system design to include details of the sensor devices, the selection of the spar-buoy as a basis for the wireless sensor buoy design, and incorporating a graphical user interface to enhance battlefield situational awareness. It continues to describe the network protocols utilized and how the network is formed; then discusses the detection of threats and how the devices share pertinent information. Chapter IV describes the wireless sensor buoy implementation and testing. It illustrates the detailed construction of the buoys, based on the design provided in Chapter III, and mounting of the sensor devices. It then describes the SIS process used to manage and

transfer the information between nodes. Finally, it presents the test phases employed to assess the validity of the WSB system. Chapter V concludes the thesis with summary remarks regarding the WSB system, reviews the observed performance, and provides recommendations for improvements in the system implementation and suggests future work that may further reinforce the concept and further improve the system design.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND INFORMATION

This chapter explores the need for perimeter security to protect vital assets. It discusses similar devices currently employed that offer protection, and the technology associated with wireless sensor networks.

A. PROBLEM DOMAIN

The problem domain explores the idea of a perimeter security and the importance of a perimeter to defending ones property. It reviews historical instances of terrorist attacks and that such attacks may occur in modern times. Current tactics, techniques, and procedures to mitigate or preclude terrorist attacks on naval vessels are discussed, and how UGS have been employed in the past to gain the tactical advantage.

1. Idea of a Perimeter Security

Much of history dating back hundreds of years implements the idea of perimeter security. Old castles used moats to impede any attacking force from gaining access to the castle walls. The moats would be constructed far enough from the castle walls to provide the desired standoff distance so that the enemy would have little to no effect; and the elevation of the walls would prove beneficial for any archers to fire their arrows down toward the enemy massed at the edge of the moat. The security that the moat afforded the castle and its inhabitants was very favorable and is comparable to other forms of perimeter security that was implemented in various means throughout history. Another example of perimeter security was applied to a fort. A fort often utilized a tall fence that surrounded the compound and protected the occupants from the attacker; this was accomplished by keeping the enemy at a significant enough distance in addition to deterring or preventing a breach of the perimeter. The fence idea is often observed in modern-day homes for the same principle of keeping intruders off of one's personal property.

Castles, forts, and modern homes are good examples of perimeter security; another good example of an application of perimeter security is prison. Prisons not only

intend to keep unwanted personnel out, but they also attempt to keep the prisoners in. Fences of prisons not only include wire or concrete, but also razor/barbed wire, electric fences, and video camera surveillance. In addition to prisons, military bases, borders, and other highly valuable installations require perimeter security and surveillance. Some critical facilities have begun to investigate emplacing concealed UGSs to further enhance the security of their perimeter. "Applied Research Associates, Inc. (ARA) has introduced an upgraded early warning monitoring system featuring 'consumable' unattended seismic sensors that can be deployed several miles away from a military base, nuclear power plant, border, or other secured area" [1]. The concept of maintaining a secure perimeter is highly relevant in modern times, just as it was in medieval times. As technology matures, so does the enemy's variety of attacking options. Facilities on land have implemented UGSs to enhance perimeter security, and as observed with the attacks on the *USS Cole* and *MV Limburg*, it is essential that perimeter security in the form of WSBs be investigated for the protection of valuable naval vessels.

2. History

Several examples exist throughout history of small units attacking naval vessels; most prominent in recent years were the terrorist attacks on the *USS Cole* in Yemen [6], the French oil tanker *MV Limburg* in Yemen [7], a Egyptian naval vessel in the Mediterranean [8]), and the attempted attack on the *USS The Sullivans* in Yemen [6]. In these cases, insurgents used small vessels to close within very short distances of target ships to conduct their attacks. The consequences of such attacks are the casualties aboard the target ships and the political implications. In addition, the attacks prove vulnerabilities to current force protection procedures and signal a victory for the terrorist organizations. In the cases of the *USS Cole* and *MV Limburg*, the Al-Qaeda terrorists utilized a small surface craft laden with explosives to approach the vessel and detonate alongside their hull. As a result of the attacks on the *USS Cole* and *MV Limburg*, 17 U.S. service members were killed and 39 were wounded, and one civilian crew member from the Limburg was killed.

Terrorist threats are a cause for concern for the security of naval vessels. Although vessels may be mobile, which reduces the likelihood of planned attacks, the USMC concept of seabasing, where seabasing is significantly less mobile, poses a greater risk of being a target for a planned terrorist attack. Terrorist attacks, while imminent in modern times, can be mitigated through enhanced force protection intelligence, training, readiness, and technology; these mitigations are always determined in an antiterrorism force protection (AT/FP) plan. The Executive Summary from the Department of Defense (DOD) *USS Cole* incident had the following finding and recommendation related to technology:

> Finding: More responsive application of currently available military equipment, commercial technologies, and aggressive research and development can enhance the AT/FP and deterrence posture of transiting forces.
>
> Recommendation: Secretary of Defense direct the Services to initiate a major unified effort to identify near-term AT/FP equipment and technology requirements, field existing solutions from either military or commercial sources, and develop new technologies for remaining requirements[9].

The Executive Summary states that new technologies should be developed to improve force protection of our sea-based assets. Mounting wireless sensors to buoys in order to enhance AT/FP may meet the intent of the recommendation.

3. Current Tactics, Techniques, and Procedures

Although the Navy has extensive security measures in place for the protection of its ships, the likelihood of a breach in security is still possible. A DOD-wide set of instructions has been developed, which is intended to provide guidance for the AT/FP of all naval property to include its ships. The Navy utilizes several references ranging from DOD Instructions (DODINST) to Navy Tactics, Techniques, and Procedures (NTTP) in order to establish AT/FP for its ships at sea. Each ship, however, compiles its own instruction to facilitate the protection of its vessel; thus, the force protection plan may differ between ships and commands. The *USS George Washington*, a United States Navy nuclear-powered aircraft carrier, drafted its instructional plan to facilitate AT/FP. Several

key elements of this instruction are annotated in this document to illustrate the current security measures that are being utilized and potential gaps, which may be mitigated with the use of wireless sensor buoys.

Currently the *USS George Washingto*n implements "security alerts" and "general procedures" to be carried out in the event of a crisis situation [10]. A security alert is an emergency situation that requires an immediate and specific response. A few of the relevant security alerts utilized by the *USS George Washington* include the following: "Boarders or swimmers are detected and suspected of making an intrusion attempt…If unable to determine intent of an inbound aircraft or watercraft" [10]. Fixed posts manned by armed sentries, Topside Rovers, fixed crew-served weapons emplacements, and dedicated Brow Cover Sentries are used to prevent an attack, though poor visual conditions may delay their reaction resulting in the attacking surface craft entering into a critically close position. The Ship's Self-Defense Force (SSDF) comprises the fixed posts:

> The SSDF is defined as armed Sailors from ship's company who provide vessel security from sabotage, damage, or compromise. The SSDF is organized and trained by the Security Officer to respond to terrorist threats, force protection and security events (including small boat attack, swimmer attack, bomb threats, demonstrators, intruders, etc.), aboard ship, and ashore as a security force, and seaward, including picket boat operations [10].

While the SSDF can mitigate terrorist threats, another limiting factor is the availability of personnel to perform the required duties. While anchored in or near a non-U.S. Navy port, the force protection conditions applicable to the *USS George Washington* only allow for a manning factor of a little over 100 personnel [10], which while substantial, considering around the clock security requirements may leave gaps. The collateral duty of being a member of the SSDF also detracts from the service members' primary responsibility of their assigned billets aboard the ship. The implementation of wireless sensor buoys would not only enhance the capability of the SSDF to provide security, but would allow the crew to focus more of their time on their primary billet responsibilities.

4. UGSs in Military Use

The use of sensor nodes to detect enemy movement is not a new concept. Originating in 1967 during the Vietnam War, UGS were utilized in an attempt to advance methods of surveillance and target acquisitions [2]. As the war progressed and little effects were achieved from high altitude aerial bombings, enemy troops were able to move around freely and conduct attacks and ambushes along vital supply routes such as the Ho Chi Min Trail. The U.S. advancement in technology and equipment led to the implementation of UGS. While not always effective, these devices had accounts of success during the Battle of Khe Sanh, where enemy troop movements were reported to the USMC's 26th Marine Regiment [2]. As the enemy began its attack, the UGS supplied limited information on mortar and artillery positions, as well as troop movement. With the information acquired from the UGSs, the U.S. Marines were able to understand the enemy's direction of movement, gain and maintain situational awareness of the enemy's whereabouts, target enemy troop concentrations and equipment, and reduce friendly casualties. The correct utilization of UGS was an essential element in the battle, which ultimately led to the U.S. Marines' victory. The U.S. military again implemented UGS in the conflicts of Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF) in the early 2000s. These devices became highly effective in the counter-insurgency fight with use in both desert and urban terrain [2]. As technology matures, so does the use and effectiveness of devices such as UGSs. Advanced modalities, improved wireless technology, and more reliable hardware and software allow UGS to provide improved Intelligence, Surveillance, and Reconnaissance (ISR), and an increase in force protection.

B. SIMILAR DEVICES TO MITIGATE THE THREAT

Before investigating the utility of UGS to deter an adversary attack, similar devices are assessed, such as sonar and unmanned vehicles that are used to mitigate the threat.

1. Underwater Sonar

Much of the development of underwater sonar occurred during the First World War under the name ASDIC (Allied Submarine Detection Investigation Committee); however, it was not until the 1930s, when several personnel from the Radio and Sound

Division of the Bureau of Engineering conducted concentrated studies to include actual field testing, did the use of sonar become essential to defeating the enemy submarine threat [3]. Although an effective tool, the application was not yielding the desired results during the early years of the Second World War. Only as a result of thorough research and statistical analysis by the National Defense Research Committee of the Office of Scientific Research and Development, were refinements to the tactics and equipment conducted and the correct implementation of sonar accepted [3]. The introduction of additional instruments that were appended to sonar made it far more capable, resulting in high rates of success [3]. This addition provided escort ships, anti-submarine surface vessels, and anti-submarine aircraft, known as hunter-killer groups, the ability to detect minefields, determine an enemy submarine's depth, provide indication of oncoming torpedoes, offer more accurate range-and-bearings, and suggest the correct moment to launch weapons [3]. The form of sonar described herein is known as active sonar.

Active sonar is a method by which a signal is emitted into the environment that reflects off of a target, specifically, sub-surface entities such as a submarine, and is then received by the searching vessel [11]. Active sonar is preferred by the Navy over passive sonar, which detects the sub-surface target by way of a receiver mounted on the searching vessel only once the target's radiated noise level exceeds that of the ambient noise of the environment [11]. The primary distinction between the applications of the two forms of sonar is that active sonar emits a radio wave that will also be detected by the target, while passive sonar simply listens and does not compromise the searching vessels' location [11]. Active sonar, however, has a longer range and can more easily detect smaller submerged vehicles than passive sonar [11].

Sonar has not only been applied to manned vessels, but since World War II, it has been employed on buoys. Known as sonarbuoys, these buoys had a sonar device attached that would report detections to a central controller and, in conjunction with local air, surface, and sub-surface vessels, would constitute a hunter-killer group, which would effectively locate and destroy enemy submarines [3]. Sonarbuoys are still in use today and utilize both active and passive sonar capabilities to detect most sub-surface threats.

2. Unmanned Vehicles

Unmanned vehicles, in addition to sonarbuoys and other sonar-equipped vessels, are also widely utilized to counter threats at sea. The varieties of unmanned vehicles employed include aerial, surface, and subsurface. These vehicles possess advanced optics and detection equipment, and facilitate extended endurance times, which significantly improve the Navy's force protection. The U.S. Navy incorporates several variants of unmanned aerial vehicles (UAVs) currently and for future intended use; some of these vehicles can provide around-the-clock coverage with an operational range of 8,000 square nautical miles [12]. The Vertical Take-off and Landing Tactical Unmanned Aerial Vehicle (VTUAV), initially deployed on the littoral combat ship (LCS), is designed to operate from air-capable ships. The VTUAV has an endurance of five hours and an operational range of 110 nautical miles from the launch site; it utilizes UHF/VHF voice communications relay [12]. It also incorporates electro-optical/infrared sensors and a laser designator, these allow the VTUAV to find, track, and designate targets [12].

Not only does the Navy utilize UAVs for protection, but it also incorporates unmanned surface vessels (USVs). These USVs are highly maneuverable with a 12-hour operational time, and designed for rapid response and high-speed interdiction in both shallow and deep water applications [13]. In addition to interdiction capabilities, the USVs are employed for intelligence, surveillance and reconnaissance, threat identification and neutralization of surface targets, communications relay, special operations forces delivery; and UAV launch and recovery [13].

In addition to USVs, the Navy also incorporates unmanned underwater vehicles (UUVs) for protection of surface vessels. These UUVs are small in size, expendable, and operated remotely due to constraints in underwater communication capabilities [14]. The primary purpose of the UUV is to detect and dispose of surface and underwater mines. It is also utilized to perform inspections, surveys, and surveillance to depths of approximately 1,000 feet [14].

C. RELATED TECHNOLOGICAL APPLICATIONS

This section discusses the concept of implementing a device such as UGS to mitigate adversary threats. It focuses on technological applications such as wireless sensor networks, specifically the sensor nodes produced by department of defense agencies that are of particular relevance in today's fight against opposing forces.

1. Wireless Sensor Networks

Computer technology has dramatically matured over the past few decades to include the introduction of the Internet and cellular phones, but only over the past decade has wireless technology and communication really thrived in the day-to-day lives of the average person. The applications of this technology are limited only by one's imagination. With the advances in wireless technology, it would benefit the military to adopt this capability, especially if the military intends to maintain the upper-hand at the tactical level of operations and ensure that they have the best level of situational awareness possible. An application of this new technology to improve situational awareness is WSNs.

A limiting factor for the military in the past has been the cost and complexity of implementing this relatively new domain of cyber communication; however, with the availability of devices so readily attainable by the general public and at such affordable prices, the military may make use of commercial off-the-shelf (COTS) products to fulfill some of its technology requirements. The wireless sensor technology, although recently easily available, does not come without challenges, as described in *Wireless Sensor Networks*:

> The design, implementation, and operation of a sensor network requires the confluence of many disciplines, including signal processing, networking and protocols, embedded systems, information management, and distributed algorithms. Such networks are often deployed in resource constrained environments, for instance with battery operated nodes running untethered. These constraints dictate that sensor network problems are best approached in a holistic manner, by jointly considering the physical, networking, and application layers and making major design trade-offs across the layers. [15]

As this technology is obtained by the military, the direct application of its uses and how it may be adapted to fulfilling the need of enhanced situational awareness is important. WSNs may be utilized to enhance protection of high-valued assets, such as troops, facilities, and naval vessels; they should be easily attainable, cost effective, and reliable to ensure maximum utilization.

2. Unattended Ground Sensors

A direct application of WSNs is UGSs. The U.S. government currently implements UGS as a tool to enhance force protection and security. The sensors are typically packaged with communication equipment and processing hardware and referred to as "nodes" [16]. The nodes are designed to be concealed and to withstand harsh environmental conditions for an extended period of time. Some of the current sensors include seismic, acoustic, magnetic, pyroelectric transducers, daylight imagers, and passive infrared imagers [16]. These sensors detect the presence of persons or vehicles and transmit the information via terrestrial radio or satellite communications to a remote station that is monitored by the user [16]. Some common applications include use by the military to support area surveillance, the U.S. Border Patrol to assist in securing the borders, and by prisons to monitor the prison perimeter fences. These applications, by using the same general concept, can be further extended to provide perimeter security for surface vessels while at anchor.

3. Defense Advanced Research Projects

Defense Advanced Research Projects (DARPA), an agency created in the 1950s, has a mission of ensuring that the U.S. is at the forefront of technological breakthroughs that pertain to national security [17]. The projects often take years to complete and get fielded. As demonstrated by start-up technology companies in the Silicon Valley area as well as other places around the world, often commercial systems of similar complexity are being developed in significantly less time. The Adaptable Sensor System (ADAPT) program is a DARPA program which specifically focuses on ISR; its goal being to deliver rapidly configured COTS hardware and software that may compete with the available commercial systems to perform specific applications [17].

A recent development under the ADAPT project is the Smart Munitions Technology, which adds mission specific hardware and software to ADAPT technology for UGS and Smart Munitions to be dropped from an aircraft, and provides sensing, location, and communication and coordination between munitions and C2 systems [18]. The research conducted by USMC Captains Bradley Palm and Ryan Richter explored implementing the Smart Munition nodes with a graphical user interface (GUI) in the form of the Mobile Situational Awareness Tool (MSAT). The MSAT allows the operator to monitor the battlefield and classify threats using a video camera that sends data to a handheld device such as a tablet or phone using either Android or iOS operating systems [4]. The nodes developed by ADAPT can be implemented for battlefield surveillance and may be capable of forming a WSN to detect sea-surface incursions in a marine environment.

D. FORMAL UNITED STATES MARINE CORPS REQUIREMENT

As the USMC continues its support of global operations, it strives to maintain an advantage "with a richer military dimension…and tactical flexibility to defeat foes throughout the littorals" [5]. The "richer military dimension' suggests the implementation and utilization of modern technology to effectively achieve the USMCs objectives in the littoral regions. The new concept of forward staging logistics in the littorals allows the USMC to respond more rapidly to any crisis abroad, to provide "the right force in the right place at the right time" [5]. These forward logistic hubs are referred to as seabases. Seabasing described by the Expeditionary Force 21 (EF-21) as:

> Seabasing incorporates the traditional naval missions of sea control, assuring access, and power projection with an increased emphasis on maneuver from the sea. By expanding access and reducing dependence on land bases, seabasing supports national global strategic objectives and provides needed operational flexibility in an uncertain world. Through seabasing we can establish expeditionary bases at sea in support of GCC requirements[5].

Seabasing reduces the logistical footprint ashore and allows supplies to be transported and distributed to more dispersed units during a more rapidly changing tempo of operations, and ultimately, supports Navy maneuver warfare [5]. The use of seabases

further counters the anti-access and area denial threat by the positioning of warships in the littorals; these warships which consist mostly of amphibious ships and enable the deployment of Marines from the sea to conduct operations ashore [5]. Aside from the advantage of easily employing Marines, the current fiscal constraints economically favor seabasing over the traditional shorebasing methods [5]. A representation of a seabase from EF-21 is depicted in Figure 1: Seabasing Concept.

Figure 1. Seabasing Concept

The above figure is a graphical representation of the Seabasing Concept which was suggested in the EF-21. Source: [5] Marine Corps Combat Development Command, "Expeditionary Force 21 Capstone Concept," (20)-March 2014.

Seabase capabilities consist of flight decks for air mobility, well decks for surface mobility, command and control suites, survivability in an anti-access environment, supporting forces for extended periods, and a flexible, rapid repositioning, self-sustaining platform [5]. An important requirement for the effective application of seabasing is force protection. The force protection will need to be increased as the forces are dispersed throughout the littoral regions creating multiple boundaries between units and extending the lines of communication, using technology and unit/individual vigilance to protect against enemy attacks [5]. EF-21 states the following force protection considerations that

are applicable to the use of technology such as the WSBs: The technology should be able to defend the MAGTF from ground, air (including counter UAS), missile, and cyber-attack. The technology should have the capability of employing passive and active systems for counter-adversary ISR deception, signature management, and decoys. [5]. The technology desired by the USMC as stated in EF-21:

> This necessitates data interoperability and direct communications between systems and collectors to enable integration of information, sensor cross-cueing, and fusion of multi-discipline/multi-source data as well as spatial and temporal visualization. Traditional and nontraditional battlefield sensors and activities should be linked by a sensing strategy that combines all sensor data, creating a Persistent ISR presence that transforms into battlespace awareness [5].

WSBs address the requirement of "data interoperability and direct communications' by using non-traditional battlefield sensors coupled with traditional battlefield equipment. The WSBs enhance ISR and ultimately battlespace awareness by defending the MAGTF from surface attacks, counter-adversary ISR deception, and eliminating the effectiveness of the adversary's use of decoys.

1. Current Shortfall

Current security measures for naval vessels are adequate, and despite the continuing threat to our valuable assets, the Navy is able to provide the required security. However, as budget cuts limit the amount of personnel on ships and as technology and developments increase obligations for the sailors, the duty of providing security stretch the responsibilities of sailors to fill multiple roles. A critical role of these sailors is security of their ship. While current threat countermeasures exist to detect underwater, airborne, and even surface advances, the threat of a small surface attack craft remains a vulnerability shortfall. Utilizing the additional WSB tool, this shortfall can be addressed; fewer sailors would be required to perform the same duty, and those providing security could do so more effectively in increment conditions and in a complete 360-degree span. The WSBs would eliminate the susceptibility of a diversionary or multi-directional attack.

2. Concept for a Solution to the Threat

The idea of creating a virtual wall around a vessel to provide security can be implemented by placing wireless sensor nodes onto spar-buoys and distributing them in a circular pattern around the vessel to be protected. The nodes would sense any breach by a small surface craft into the security area surrounding the vessel being protected. Once detected, the nodes would notify the base station monitored by the watch crew located on the vessel of the impending threat, and the watch officer could then take the appropriate action. The base station may display the threat on a handheld device using a GUI and map overlay similar to the MSAT developed by Palm and Richter [4]. The nodes may also alert the watch crew to several types of attacks conducted by slow moving surface vessels. A thorough testing plan would need to be conducted in order to prove the worth of such an implementation of the devices. The scope of this thesis will prove the concept of effective communication of the wireless sensor network in order to validate the proposed configuration. The proposed topology is illustrated in Figure 2.

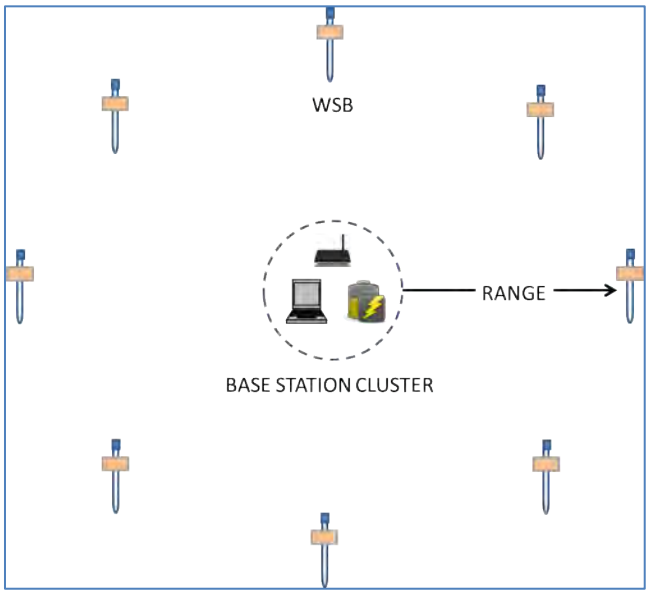

Figure 2. Proposed Topology

3. Possible Use Case and Employment

The wireless sensor buoys are designed to detect breaches in the perimeter by small surface vessels; they may be effective in both deterring a standard attack by a single craft or multiple attacks by surface vessels.

a. Standard Attack

A standard attack would be described as a single surface craft, much like the type that conducted the attack on the *USS Cole*, which could be loaded with high explosives and slowly navigated toward the target vessel for a suicidal "kamikaze" style attack.

b. Diversionary Attack

A diversionary attack in this scenario is an attack whereby a small craft purposely breaches the perimeter and alerts the watch crew, which in turn would alert the security of the naval ship to defend against the advancing threat. While the security crew is focused on the current danger, a secondary or tertiary threat may attempt to covertly breach the perimeter on the opposite side of the vessel. Without anyone noticing, the additional threat may conduct a successful attack on the targeted ship. The advantage of utilizing a WSB network would provide constant 360 degree perimeter notification of any threats that may be approaching. Assuming that the watch crew is monitoring the network, the probability of a successful diversionary attack is almost zero.

E. SUMMARY

This chapter has discussed the concept of perimeter security and its implementation throughout the ages, and how it can be relevant to naval security. It has been identified that the current threat of a small surface-vessel suicide attack is relevant in modern times, as indicative of recent historical events. With the current threat, present AT/FP doctrine suggests that additional measures should be emplaced to mitigate terrorist attacks against naval vessels. In addition, a system that alleviates the collateral duties of sailors and allow them to focus more on their primary duties and responsibilities may achieve a greater combat readiness for the U.S. Navy. Devices such as sonar can detect sub-surface threats and unmanned vehicles may identify threats above the surface;

however, additional tools utilizing modern technology and equipment could further diminish attacks against high value U.S. vessels by providing additional advanced warning. WSNs in the form of the UGSs developed by DARPA addresses the necessary security concern. The USMC has explicitly stated the need for enhanced security during future operations in the littoral regions; WSBs addresses the requirement by using existing devices that leverage COTS components to increase situational awareness and enhance AT/FP perimeter security for military vessels and seabases. In Chapter III, the concept of employing a wireless sensor system on buoys is presented and specifics of the network infrastructure are discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SYSTEM DESIGN

This chapter explores how this WSN, consisting of wireless nodes attached to buoys, relay the information to the base station monitoring device located on the vessel being protected. It describes the ADAPT UGS/Smart Munition prototype designed by DARPA and the selection of the spar-buoys required to provide a base for the nodes. The chapter then briefly discusses the use of an application server and graphical user interface to implement the MSAT, which will be used in future testing, and the final employment of the overall WSB system. Chapter III also explains the connectivity of a WSN and specifically the capabilities of the network used by the ADAPT nodes.

A. SYSTEM DESIGN CONCEPT

The concept of the WSB system was to utilize existing COTS technology implemented in the ADAPT sensor nodes and mounting the nodes to buoys for the purpose of creating a WSN; the network then relays information to a central base station monitoring device located on a naval vessel. The final system would report breaches in the security perimeter by detecting foreign objects with its sensors and reporting the detections to neighboring nodes and to the base station aboard the vessel being protected. The reports would generate data that would be translated to information and be displayed graphically on a mobile device. Upon inspection of the information, the appropriate force protection procedures by the SSDF would be enacted and the threat neutralized. Figure 3 depicts the scenario described.

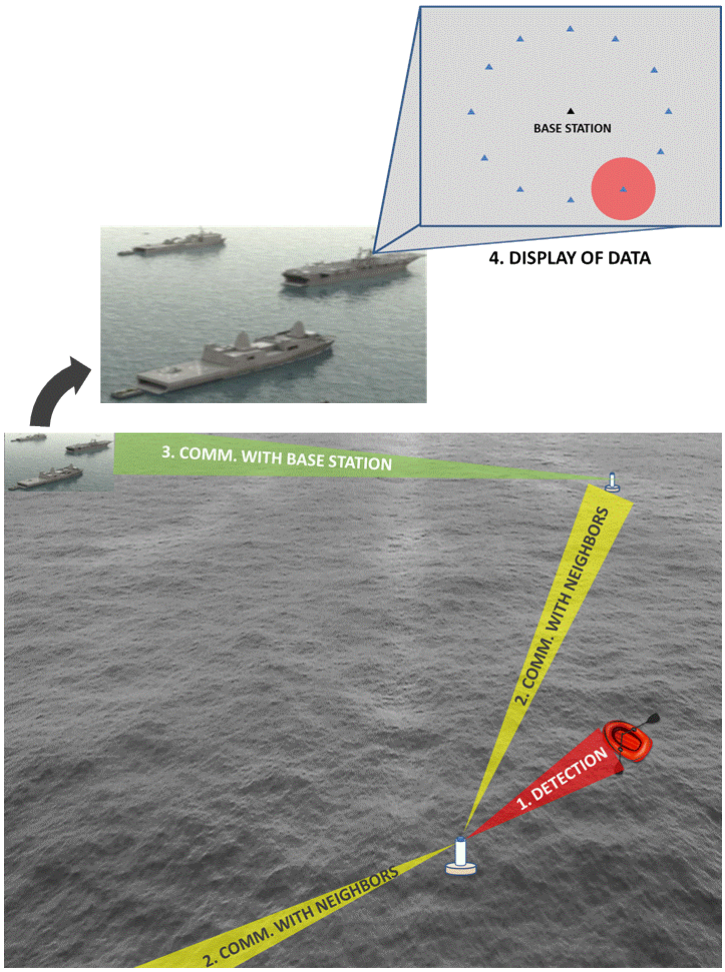

Figure 3. System Design Concept

Adapted from: [5] Marine Corps Combat Development Command, "Expeditionary Force 21 Capstone Concept," March 2014

The scenario in Figure 3 illustrates how the WSB concept, combining existing technologies in the form of ADAPT sensor nodes and spar-buoys, may be implemented to provide advanced warning and improve force protection for naval vessels and seabases.

1. Sensor Nodes

To detect incoming threats, the sensor nodes form the essential means of alerting the operator of any enemy presence. The sensor nodes may be equipped with multiple modalities to detect an intrusion; some modalities currently in use include sonar, seismic,

acoustic, camera, and passive infrared (PIR). Sensors suggested for use in future nodes include laser range-finding, laser scanners, and LiDAR (Light and Radar). Since the prototype node produced by ADAPT contains PIR, and that several nodes were readily available for utilization, it was decided that the ADAPT version-1 nodes would be utilized for the testing of this thesis. The current nodes include a global positioning system (GPS) receiver, the receiver allows for the location of the node to be determined [18]. They have an onboard power source that gives the nodes the ability to function for 14 days. All processing of the node is conducted onboard the sensor node itself, rather than by a central processing station; this allows for a scalable network where additional nodes can be added to or removed from the perimeter without having an adverse effect to the bandwidth of the entire network [4]. Since the nodes utilize COTS technology, they are inexpensive and can be considered expendable and easy to replace if necessary. The nodes are lightweight and small, which is an advantage for storing aboard naval vessels where the limited space available is a significant logistical concern.

Other UGSs such as the ARGUS perimeter system [19] are in use only in a ground-based capacity and are available; however, since the DARPA built ADAPT UGS were on-hand requiring no additional acquisition, it was decided that these nodes would be utilized to prove the concept of mounting sensor nodes on buoys to form a WSN. A concern of the ADAPT UGSs was the PIR sensors; it was assumed that the sensors would not function effectively as the motion of the water may cause the sensors to be "tripped" inadvertently, alerting the operator to a perimeter breach and a false-reading. While a substantial concern, the scope of the thesis was merely to prove the concept of a node mounted on a buoy with the ability to communicate to other nodes and to a base-station wirelessly. This concept would prove the validity of a WSB system that could be incorporated into a network to form a security perimeter for naval vessels.

The ADAPT UGS/Smart Munition prototype was a DARPA program that was initiated in 2012 with the scope that included a development effort divided into three tracks [18]. The first track consisted of ADAPT investigating the use of COTS technology for use in sensors and smart munitions; for the second track DARPA undertook the smart munition technology development which included adding mission

specific hardware and software to ADAPT technology providing sensing, location and communication/coordination between munitions/C2 systems; finally, the third track consisted of replacing current air-dropped munitions with the DARPA smart munition technology.

As a result of the three tracked development effort, these nodes were capable of being hand placed, airdropped, or dispersed via artillery fire [18]. Although designed for the replacement of munitions and landmines, these nodes could also be applied as a detection system in a perimeter wireless sensor network to protect ships; this application would require the sensor nodes to be placed a small distance above the surface of the water on a floatation device such as a buoy. By implementing these tools and the perimeter security concept, the requirement of the EF-21 for additional protection for naval vessels operating in the littoral regions can be attained.

The ADAPT smart munitions prototype is comprised of several essential components which include a plastic housing with both ground and WiFi antennas, hardware components to include a GPS antenna, sensor devices consisting of a PIR sensor and two cameras, a battery pack, an Android operating system, and several applications and protocols [18]. A cutaway view of the DARPA smart munition prototype hardware is depicted in Figure 4.

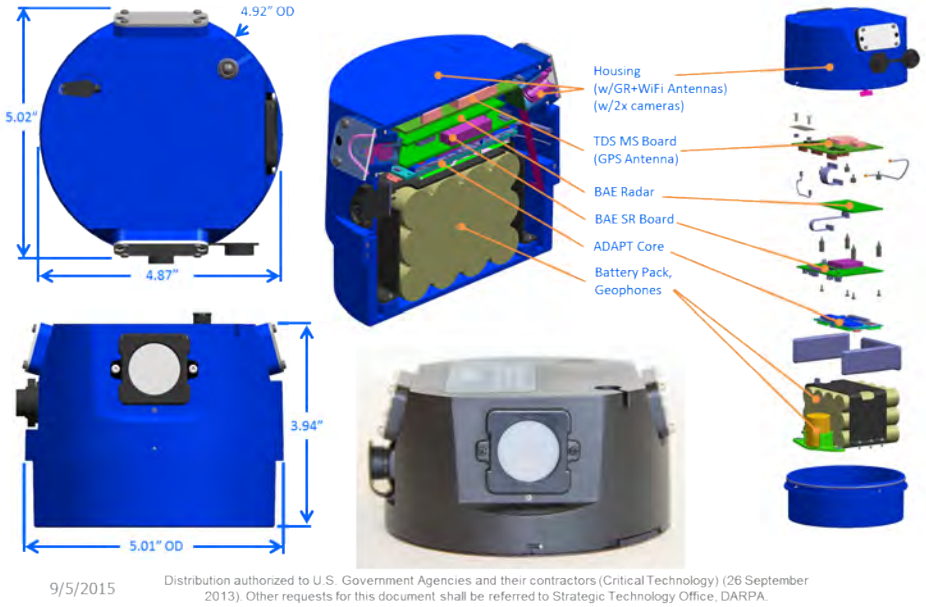

Figure 4. DARPA Smart Munition Prototype Cutaway

Figure 4 represents DARPA's smart munition prototype developed by ADAPT using COTS components. The figure displays the sensor top, side, and cutaway views. Source: [18] T. Hammel and M. Rich, "ADAPT smart munitions: Summer camp final demonstration," presented at Naval Postgraduate School, Monterey, CA, Sept. 26, 2013, PowerPoint
pp. 8.

a. Housing

The housing of the ADAPT sensor node is comprised of two primary pieces manufactured from hard plastic, utilizing rubber seals at all the joining connections to provide a degree of water resistance. It is approximately four inches in height with a diameter of approximately five inches on the upper portion and approximately 4.9 inches on the lower portion; the small difference in diameter thickness was vital to seating the node securely onto the spar-buoys. The lower portion contains the battery pack while the upper portion contains the remainder of the components.

b. Core Hardware

The ADAPT core hardware consists of a Qualcomm MSM8960 Snapdragon System-on-a-Chip Dual Core processor, graphics processing unit, GPS Processor, and 3G/4G modem [18]. The core has a removable MicroSD card for persistent storage, and core also

includes WiFi, Bluetooth, Cellular, and GPS antennas. The core hardware allows for external input/output (I/O) devices such as the sensor, communication, security, memory, and actuator to be utilized.

c. Sensors and Cameras

The ADAPT nodes contain both a PIR sensor and two cameras. The PIR sensor is capable of detecting moving objects out to ranges of approximately 50 meters [4]. While larger objects such as vehicles may be detected at this range, humans sized objects are only detectable at ranges of approximately 20 meters. The PIR is sensitive and a concern for detection of objects while on the ocean surface as it may be inadvertently triggered by the movement of the surf. Other sensors such as LiDAR or laser ranging devices should be investigated. In addition to the PIR sensor, each node contains two cameras on opposite sides of the device. The intent of the cameras is to confirm whether the object detected by the PIR sensor is a threat or not; this can be conducted using either still imagery or video [4]. Due to errors in the software, the cameras were inoperable and not used during the conduct of this thesis work.

d. Power Consumption

The ADAPT nodes are powered by rechargeable lithium-ion battery packs which are housed in the lower portion of the node. Six different power states are implemented to conserve energy and are managed by an Android operating system [18]. These power states are depicted in Table 1.

Table 1. Power States

State	Description	Power (mW)	Duty Cycle	Lifetime (blue node) (days)	Lifetime (1/3 battery) (days)
Vigilant	PIR enabled. MSM sleeping. Ground radio running with 1 receive slot.	80	0.934	62.5	20.8
Characterization	PIR enabled. Seismic software characterization. MSM enabled. SAS running with 1 receive slot.	412	0.040	12.1	4.0

State	Description	Power (mW)	Duty Cycle	Lifetime (blue node) (days)	Lifetime (1/3 battery) (days)
Tracking	Sensors fully operational. Seismic software characterization. SAS broadcast slots enabled. WiFi overwatch enabled.	568	0.016	8.8	2.9
GPS On	CPUs idle. GPS location query at 1s interval.	804	0.008	6.2	2.1
Video On	Video recording. Sensors fully operational. Seismic software characterization. SAS broadcast slots enabled. WiFi overwatch enabled.	1556	0.003	3.2	1.1
Full	Both CPU's at maximum load, all radios enabled and transferring data	3156	0.000	1.6	0.5
TOTAL		110	1.000	45.2	15.1

Table 1 represents the six ADAPT node power states. Source: [18] T. Hammel and M. Rich, "ADAPT smart munitions: Summer camp final demonstration," presented at Naval Postgraduate School, Monterey, CA, Sept. 26, 2013, PowerPoint pp. 15.

When deployed the nodes remain in the "vigilant" power state waiting for an intrusion and listening for any reports from their neighbors [18]. When neighboring nodes transmit information of a local intrusion, the node transitions to the "characterization" power state; the PIR sensor is on and the processor is enabled allowing for quicker detection of threats. After an intrusion is detected the node transitions to the "tracking" power state with all sensors active; WiFi is also enabled in order to transmit data directly to the base station, and the ground radio is implemented to transmit information to the neighbors via the SAS protocol [18].

The "GPS on" power state is enabled during the startup and remains on "for one hour to allow the network to stabilize and acquire locations for all neighboring nodes" [4]. Every four hours this state is activated for a period of ten minutes to re-acquire location data. In GPS denied environments the nodes acquire locations by deriving a center of mass from neighboring nodes [4]. The "video on" power state is activated once an intrusion occurs and is used to assist with classifying the moving object. During the "full" power state, all sensors are active, all forms of communication devices are active, and the GPS is functioning [4].

e. Operating System

The operating system utilized in the ADAPT nodes is an Android operating system which was custom configured and optimized to achieve low power consumption that extends the operating life cycle of the nodes [4]. The operating system implements a Linux kernel and the C programming language.

f. Node Software

The node software for the ADAPT nodes incorporates a Shared Information Space (SIS) process which enables the nodes to share data between each other using a small database [4]. Communication between nodes is via a 900 MHz ground radio using the Scheduler and synchronous/asynchronous (SAS) medium access control (MAC) protocol processes [4]. The system clock is managed by the RTC Real Time and System Clock Synchronization process. Applications built into the software control key tasks such as node locations, PIR sensors, detection data, and tracking data. The software also includes drivers for the field programmable gate array (FPGA), ground radio, and PIR sensors [4].

2. Buoy's

To establish a perimeter of sensor nodes around a naval vessel or group of naval vessels, a means to support the sensors was required. Several options were investigated to support the nodes, which included floating security barriers, as depicted in Figure 5, containment barriers in Figure 6, and buoys. The option to mount the nodes on buoys was selected because of the ability to customize the topology depending on the formation of the ships, and more specifically to allow amphibious traffic to pass without obstruction as would be the case if the floating security barriers or containment barriers were to be utilized.

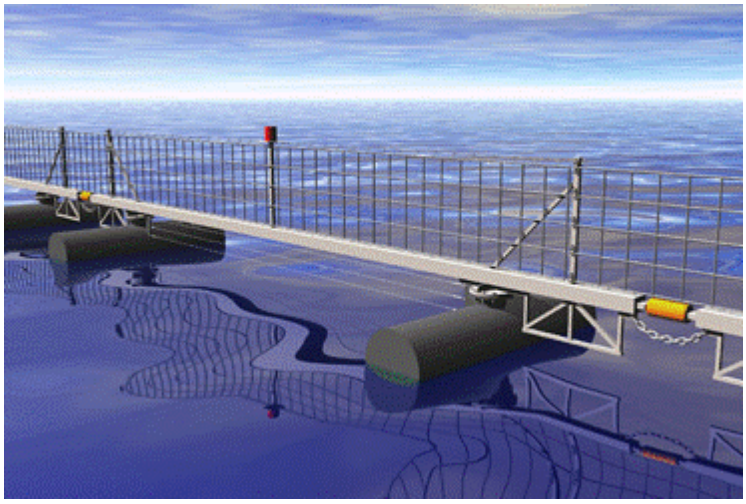

Figure 5. Floating Security Barriers

A Computer Aided Design of the Floating Security Barrier which was considered for mounting the sensor nodes upon. Source: [20] M. Kane. (2009). C.A.D./Mapping Services, Inc. Harbor Offshore, Inc. [Online]. Available: http://www.cadmappingservices.com/HARBOR2.html

Figure 6. Containment Barrier

The figure represents an example of a Containment Barrier that is used to prevent the spread of oil, fuel, silt, and debris. This was an option considered for mounting the sensor nodes upon. Source: [21] Equipment Items: Containment Systems. (2015). Global Diving & Salvage, Inc. [Online]. Available: https://www.gdiving.com/node/124

Figures 5 and 6 display options considered for mounting the wireless sensors upon; however, the decision was to utilize buoys. The floating security barrier was too large and cumbersome to be rapidly redeployed for the dynamic nature of amphibious operations in the littoral regions, and the ability to store the system aboard a naval ship was a significant concern. While the containment barrier option was a viable solution since it could be easily stored aboard a ship without consuming excess storage space, it still required the use of buoys to prevent the barrier from drifting with the ocean currents. A detriment to the containment barrier option was that any movement by friendly forces in and out of the perimeter would be limited and reduce the mobility of smaller amphibious operations.

The buoy option would facilitate ease of storage aboard Navy ships in addition to allowing freedom of movement of the smaller amphibious craft through the perimeter. With the concern of storage space, the spar-buoy design was selected by Oceanographers Commander (retired) John Joseph, and Lieutenant Christopher Merriam from the Naval Postgraduate School. An additional advantage of utilizing the spar-buoys would enable the nodes to be mounted at a specified height above the surface of the water, which would account for the ocean swell and increase the possibility of unimpeded detections. The modifications to the standard spar-buoy design in order to facilitate the wireless sensor node were produced by Commander Joseph, Thomas Rago, and Lieutenant Merriam; these persons also all assisted in the construction efforts. An example of a standard spar-buoy is represented in Figure 7.

Figure 7. Standard Spar-Buoy

The figure represents an example of a Standard Spar-Buoy that provides the required height above sea water. This was the option selected for mounting the sensor nodes upon. Source: [22] Spar Buoy. (n.d.). *Wikipedia*. Available: https://en.wikipedia.org/wiki/Spar_buoy. Accessed Nov. 3, 2015.

The modifications suggested by the Oceanographers are depicted in Figure 8. Note the addition of the ballast provides the additional stability required by the sensor node. Also of interest is the location of the anchor point, which limits the tipping of the buoy in high wind and ocean current conditions. The prototype had the anchor point location at the water surface line; however, the final version relocated the anchor point location to the spar-buoy center of gravity.

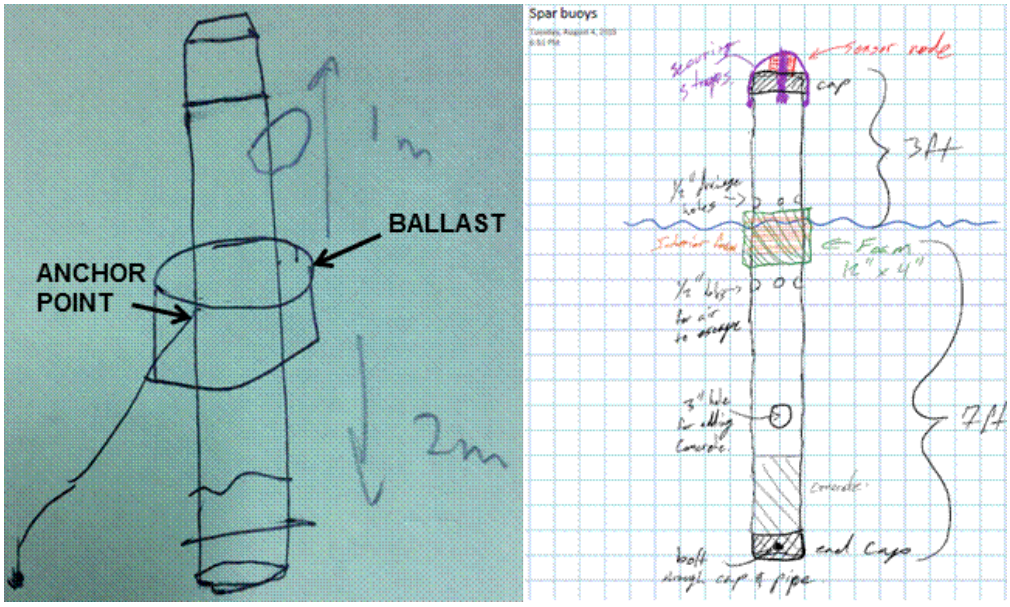

Figure 8. Modified Spar-Buoy Design

The modified design proved successful during the Phase III test. Further details of the design and the construction are discussed in Chapter IV. A primary consideration in the design was a low cost, ease of manufacture, and rigidity that would enable the spar-buoy to withstand the increment conditions of the ocean environment. Adapted from: [23] J. Joseph, C. Merriam, "Initial Modified Spar Buoy Design," unpublished.

3. Application Server and Graphical Display

The extent of the design covered in this thesis is the WSB and the ability for it to communicate wirelessly in an ocean setting. Future extensions to the system would be the inclusion of the MSAT. The MSAT developed by Captains Palm and Richter for detecting ground intrusions provide a graphical display for the operator to monitor the data processed from the sensor nodes. This effective tool allows the user to visually observe the nodes on a mobile handheld device such as a smartphone or tablet, and receive alerts graphically to a breach in the perimeter significantly increasing situational awareness [4]. The MSAT utilizes a web-based HTML5 front-end application enabling compatibility with both Apple and Android devices. The graphical display incorporates a map that can be scrolled, zoomed, and rotated with the sensors overlayed to indicate intrusions. The intrusions are displayed as flashing graphics or lines displaying the tracks of targets as they move through the security area. Audible alarms and vibrations could be utilized as a redundant feature to further enhance the situational awareness. A pop-up window is included

in the application to provide video or still images of intruders from the built in camera onboard the node, which would visually confirm the threat [4]. A representation of the MSAT display is illustrated in Figure 9.

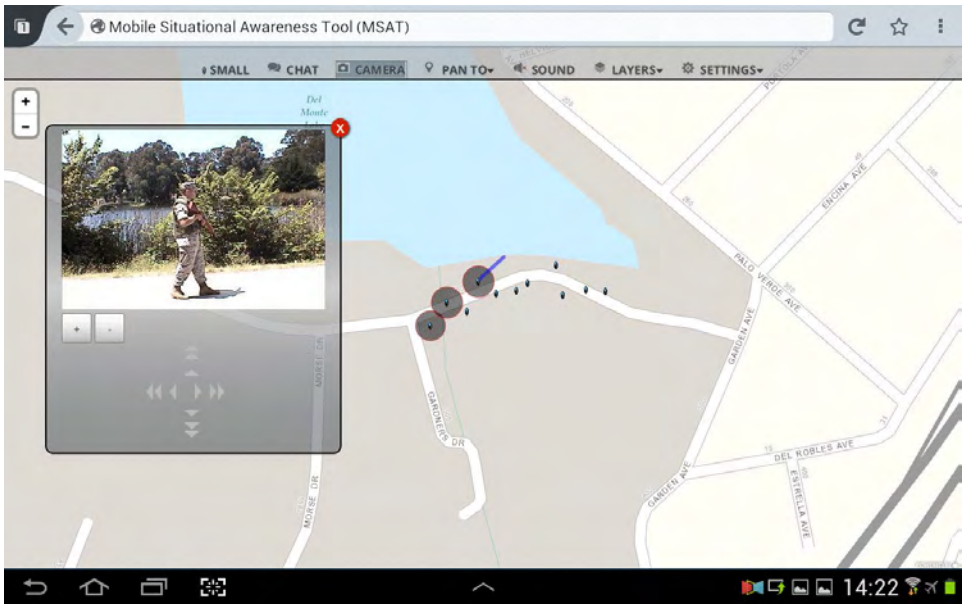

Figure 9. MSAT

The figure represents an example of the MSAT developed by Palm and Richter. This tool can be implemented with the WSB design to further enhance situational awareness. Source: [4] B.C. Palm and R.P. Richter, "Mobile situational awareness tool: unattended ground sensor based remote surveillance system," M.S. thesis, Dept. Computer Science, Naval Postgraduate School, Monterey, CA, 2014, p102.

The MSAT was not included in the testing of the WSB during this thesis due to issues with the previously established server and that it was not an essential requirement in the scope of this research. It is suggested that the implementation of this tool be utilized for future use applications and testing.

4. Overall System Design

The overall system design consists of wireless sensor nodes mounted on spar-buoys and distributed in a circular network surrounding a naval vessel. The buoys are anchored using a 25lb anchor. The nodes communicate amongst each other and report breaches in the perimeter, reporting back to the base station and the watch crew aboard

the ship monitoring the network. The WSB system consists of the sensor nodes, spar-buoy, base station computer, router, MiFi hotspot, Access Point (AP), battery, and setup computer. The following equipment was utilized to enable the WSB system to function: The sensor node in Figure 10 features the hardware, software, sensors, and power source required to detect the threat.

Figure 10. ADAPT Sensor Node

The node, constructed by ADAPT, will be described in further detail in Chapter IV. The spar-buoy that mounts the sensor node is depicted in Figure 11. The buoy is constructed of PVC pipe and utilizes polyethylene foam for additional ballast. The buoy is also equipped with a 10lb weight to provide stability and an anchor to prevent drifting.

Figure 11. Modified Spar-Buoy

The Spar-Buoy prototype image featured in Figure 11 was captured during the Phase III test.

Details of the spar-buoy construction will be covered in greater detail in Chapter IV. The base station computer receives the data, via WiFi 802.11n, that the nodes collect and provides feedback to the user of the network to include node locations, detections, and tracks contained in the SIS process. The base station utilized was a 64-bit Intel Core i7 with a 1.80GHz Quad-Core processor running Ubuntu 12.04 LTS. For the programming of the nodes, to include establishing the SIS version and mission parameters a Lenovo ThinkPad T510 with a dual 2.67 GHz Intel Core i7 CPU and 4 GB RAM running a 64-bit version of the Ubuntu 12.04.4 LTS operating system was utilized. The base station running the SIS process is depicted in Figure 12.

Figure 12. Base Station Computer

The base station connects to the network via a Dell TrueMobile 2300 router, a Verizon MiFi hotspot, and a Teletronics International Inc. EZ Platform repeater operating at 2.4GHz. The router, MiFi device, and repeater are illustrated in Figure 13.

Figure 13. Router, MiFi Device, and Repeater

The MiFi Jetpack (center) used to connect to the server for use with the MSAT, and the Dell router (left) for network redundancy.

The equipment in Figure 13 forms the infrastructure to connect the sensor nodes to the base station and provide the data to the operator. Figure 14 represents the host connections to the network.

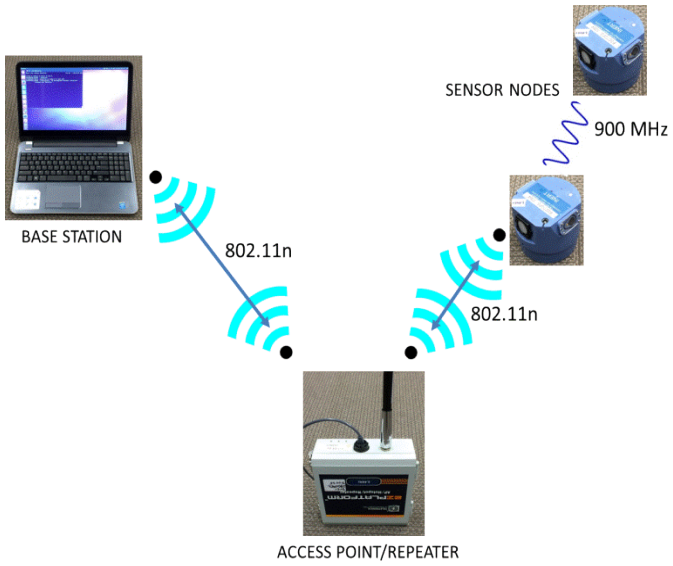

Figure 14. Host Connections

To deliver the necessary power in order to facilitate the operation of the system, a Yeti 400 solar powered portable battery was utilized. The Yeti 400 depicted in Figure 15 is able to provide power to the system for several hours and weighs approximately 29lbs [24]. For the final implementation of the WSB system, onboard ship power can be utilized which would provide indefinite power to the base station cluster.

Figure 15. Yeti 400 Power Source

The Yeti 400 power source was fundamental for testing during this thesis; however, future testing would not require it if sufficient power was available from onboard a vessel. The complete base station cluster consisting of the base station computer, router, MiFi hotspot, Access Point (AP), and Yeti 400 battery is depicted in Figure 16.

Figure 16. Base Station Cluster

The base station cluster illustrated in Figure 16 is operated by the user "watch crew" and would be located in the naval vessel that requires protection. With the complete WSB system implemented, the operator would be able to monitor the security perimeter and be alerted to any enemy threat that may breach the vicinity.

Figure 17. Final Spar-Buoy

The spar-buoy has both the node and the anchor attached, and is ready for deployment.

The overall configuration would consist of a circular perimeter of WSBs around a base station cluster located centrally on the vessel being protected. The quantity of buoys is dependent on the effective range of the communications protocol in use, the modalities, and the location where the vessel is at anchor.

B. NETWORK

The network is the essential factor of the WSB system. It requires reliable communication protocols to report information from the sensor nodes to the watch-stander monitoring the base station computer. The network facilitates information transfer between the nodes and reports threats that are detected by the nodes onboard sensors.

1. Communication Protocol

The WSB network utilizes both WiFi 802.11n to communicate between the base station and the ADAPT sensor nodes, and the ADAPT nodes onboard 900 MHz radio, which uses the SAS MAC protocol [18].

a. 802.11

The ADAPT nodes make use of the 802.11n wireless protocol. The 802.11 protocol is a protocol created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802) and allows for wireless communication. It operates in various frequency bands to include 2.4 and 5 GHz [25]. The 802.11 protocol is divided into several classes known as standards. The standards each have different performance characteristics. The 802.11n standard incorporates multiple in, multiple out (MIMO), "which transmits multiple streams of data on different antennas in the same channel at the same time and then recombines the streams at a receiver that also has multiple antennas and radios" [25]. 802.11n also makes use of both the 2.4 and 5 GHz frequency bands; however, for testing during this thesis only the 2.4 GHz band was utilized.

The 802.11n standard has some limitations. The most concerning limitation is the range; According to WiFi Planet 802.11n, although provides a greater range than the older 802.11g, is only capable of effective communication up to an average distance of 250 meters [25]. Although the range is variable depending on the router configuration and environmental conditions, the results determined during testing suggest a range of 200 meters using the current system configuration is attainable.

A further limitation using the 802.11n on the 2.4 GHz frequency band is the potential of noise. Since the 2.4 GHz frequency band only utilizes three overlapping channels, should other devices be operating in the same frequency band, a chance for overlapping exists which would affect communication [26]. While conducting tests in a secluded environment such as the open ocean the 2.4 GHz was effective; however, for future tests where substantially more devices using the frequency band may be present, the use of the 5 GHz frequency band may be preferred. To further enhance range and reliability over utilizing 802.11n, a modern more advanced protocol standard such as 802.11ac or 802.11ay should be investigated. Other devices, such as ChipSAT, are an alternative to improving communication between the nodes and the base station.

b. 900 MHz Ground Radio Using SAS

The ADAPT nodes communicate wirelessly between each other via a 900 MHz ground radio. The ground radio communication utilizes the SAS MAC protocol which

implements both time division multiple access (TDMA) and frequency division multiple access (FDMA), and are scheduled locally by the nodes as required [18]. The idea behind utilizing both TDMA and FDMA is to most efficiently utilize the radio spectrum. The FDMA takes the frequency being used and divides it into sub-frequency slots, the TDMA then further divides the sub-frequency slots into various time slots; the ADAPT nodes utilize the time slots in a range of 4.6 to 8.6 milliseconds [18].

The nodes conduct a "three message handshake," which could either be initiated randomly or by a message from a neighbor; the process continues forever, and the random rate drops over time and with the reduction of the number of neighbors [18]. The three message handshake is depicted in Figure 18.

Slot	Node A	Node B	Node C
a		* "I'm listening on slot b" *	
b	"I'm listening on slot a" "Will you be my neighbor?"		
c			
a		I'll be your neighbor.	
b			
c	* "I'm listening on slot a" *		
a			"I'm listening on slot c" "Will you be my neighbor?"
b			
c	I'll be your neighbor. "B is listening on slot b"		
a			
b			"I'm listening on slot c"
c		"I'm listening on slot b" "Will you be my neighbor?"	
a			
b			I'll be your neighbor.

Figure 18. Three Message Handshake

The "three message handshake" conducted between three ADAPT nodes using three different slots. Source: [18] T. Hammel and M. Rich, "ADAPT smart munitions: Summer camp final demonstration," presented at Naval Postgraduate School, Monterey, CA, Sept. 26, 2013, PowerPoint pp. 22.

The data is transmitted in a bundle format containing at least one packet of variable type and length. The bundle contains a "bundle header," "packet header," "packet data," and an "ack." The bundle format is illustrated in Figure 19.

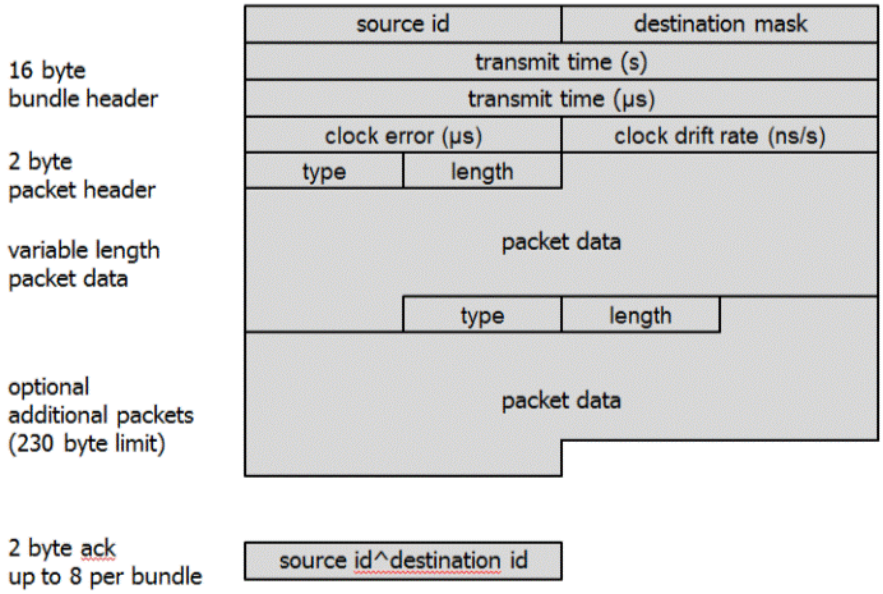

Figure 19. SAS Bundle Format

Figure 19 shows the bundle format for the SAS protocol. Source: [18] T. Hammel and M. Rich, "ADAPT smart munitions: Summer camp final demonstration," presented at Naval Postgraduate School, Monterey, CA, Sept. 26, 2013, PowerPoint pp. 22.

2. Network Formation

A network formation is essential to facilitating the operation of the WSB security perimeter. In order for the network to form the nodes are required to discover their neighbors, synchronize time, and determine their location. The nodes discover their neighbor by conducting the three message handshake and share information of previously discovered neighbors; this increases the time of the discovery process. The SAS protocol however limits the number of neighbors to eight [4]. The importance of synchronizing time is so the nodes can correctly communicate using the TDMA of the SAS protocol. The nodes acquire their time from the GPS receiver located in each node; however, this method proved only partially reliable. To ensure the correct time was achieved, the SAS

implements an over-the-air (OTA) time synchronization algorithm and updates any clock errors or clock drifts [18]. The locations of the nodes are determined primarily by GPS and also an estimate from neighboring nodes using a center-mass calculation [4].

3. Threat Detection

The ADAPT nodes are equipped with PIR sensors for detecting objects which are then shared with neighboring nodes and relayed to the base station. As the PIR sensors of three consecutive nodes detect an object a track is created. The triangulation of the object by the nodes facilitates the bearing, speed, and location that form the track. The information is then shared with neighboring nodes and ultimately the base station monitored by a human controller. The PIR sensors function by:

> electronically sensing infrared light given off by an object moving through the sensor's field of view. Any object, with a heat differential in respect to the surrounding ambient temperature, moving in front of the node's PIR sensor would trigger a detection event. Upon a detection being triggered by the PIR sensor, the node would process the event—determining whether this detection was part of a sequence of detections from other nearby nodes (i.e., a track) and which neighbors to share the new detection with based on sharing-parameters set on the nodes. Nodes were set to send detection and tracking information with neighbors located within a 100 meter radius of the event[4]..

The PIR sensors are completely valid for ground based detection while the nodes are static; however, the concern of false detections while the nodes were mounted on buoys upon the ocean surface was confirmed during the tests conducted as explained in detail in Chapter IV. The PIR sensor has a detection range of only a few meters and varies depending on heat differentiation. On average the PIR sensors would detect human objects at a distance of 20 meters. To increase the detection ranges and reliability other sensors such as LiDAR or laser ranging devices should be investigated. LiDAR could provide a 2-D horizontal scan or 3-D scan if actuated. The LMS 200 LiDAR produced by SICK has a 180 degree field of view and can range up to 80 meters [27].

4. Data Sharing

The received data from the node is stored in separate tables on its operating system using the SIS database [18]. As neighbors relay data over the SAS ground radio protocol, the data is added to the existing tables on the neighboring nodes. The nodes determine if the data received is important and forwards the information to other neighbors; this process allows critical data to be transferred across the network. The nodes then use WiFi 802.11n to send the critical information to the base station on port 10000 [4]. The operator on the base station is also able to communicate with the nodes and issue specific instructions or modify the tables.

5. WSB Network Topology Concerns

Standoff (the distance of the target from the vessel) is vital to providing the required security. The WSB system would need to support a topology capable of providing detections of an incoming threat and notifying the base station in a timely manner and at a substantial distance to where the SSDF may be able to react and prevent the attack. This distance is variable and dependent on the speed and vector of the incoming threat and the reaction time of the SSDF. Further testing and training is necessary in determining the optimal distance that the nodes should be deployed from the vessel. As the radius distance increases, so does the requirement for additional node/spar-buoys, and redundant/more reliable communication. For the purpose of the tests conducted in this thesis, a distance of 90 meters was assumed. The 90-meter distance was selected since the nodes were known to reliably communicate at that distance, and a small craft approaching at a slow speed should provide the time necessary for the SSDF to react. Alternate topologies could be investigated to include a multi-layered perimeter which would provide a greater standoff and create redundancy in the network should a node fail or be compromised. The multi-layered topology also reduces the possibility of any gaps generated between nodes placed on the perimeter. Gaps may be produced either by failing nodes or by large ocean swells.

C. SUMMARY

In this chapter the concept of the WSB system was discussed. The WSB idea of mounting ADAPT sensor nodes to buoys for the purpose of creating a WSN, and then relaying information to a central base station monitoring device located on a naval vessel was addressed. The components of the ADAPT UGS/Smart Munition prototype were analyzed to include the housing, hardware, sensors, power states, operating system, and software essential to the performance of the node as a wireless sensor. The selection and design of the spar-buoy was investigated as it pertained to the proper implementation of the ADAPT nodes to form the WSN. The MSAT developed by Palm and Richter was discussed as an additional tool for use with the WSB system; and the overall system design was described.

The 802.11n WiFi and 900 MHz ground radio communication capabilities were addressed to include limitations with the current design. The formation of the network was described and how the nodes sense and communicate threats by transmitting their data. Finally, concerns with the WSB network topology were stated. In the following chapter, the construction of the spar-buoys, mounting the ADAPT nodes, the equipment utilized to establish the wireless network, and the SIS program is presented. Further presented in the following chapter are the tests conducted to confirm the validity of the WSB system.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. WIRELESS SENSOR BUOY IMPLEMENTATION AND TESTING

To explore the validity of the sensor buoy concept, a four phase test was conducted which included two dry-land tests to confirm signal ranges and topology configuration, and two ocean tests to confirm the buoy functionality and how the WSB network would perform on the ocean surface. The equipment utilized to conduct the tests included the ADAPTv1 sensor nodes, spar-buoys, base station computer, router, Teletronics International Inc. 2.4GHz repeater, Yeti 400 portable battery, and setup computer.

A. BUILDING THE BUOYS

The modified spar-buoy consisted of a 10-foot long, 6-inch diameter polyvinyl chloride (PVC) pipe typically utilized for irrigation purposes. The pipe-based buoy was designed to provide approximately a one meter height above the water surface for the node. The relevance of the one meter height was to minimize the obstruction of ocean surf prevalent in littoral regions and still remain close enough to the surface to detect intrusions. Approximately 1/3 of the buoy was above the surface, while the remaining 2/3 was below the surface to account for wind and current effects. In addition to the PVC pipe, polyethylene foam ballast was utilized to provide the buoyancy necessary to maintain a steady platform; polyethylene is often used for buoyancy in marine equipment and its buoyancy factor is well studied. Various stainless and galvanized steel nuts and bolts were incorporated into the design since rust would be a concern for the buoys over a substantial length of operation time. A 10lb weight was attached to the bottom of each buoy to aid in the stability and was connected to an end cap for ease of manufacture. To ensure that the buoys remained in their designated positions once deployed, a 25lb anchor was attached to each of the buoys.

To test the design a prototype was constructed. The initial design utilized concrete at the bottom. Working with the concrete was difficult as the 10lb weight requirement fluctuated due to water evaporation after the wet concrete was mixed and poured. A

modification to the prototype replaced the concrete with a 10lb plate typically utilized by body-builders for weight lifting; this ensured accurate weight and was significantly easier when manufacturing the buoys. Initially, the anchor was designed to be connected at the water line; however, after testing the prototype it was determined that the anchor connecting point needed to be positioned at the center of gravity of the buoy. The reason for this revised position was to eliminate drag produced by ocean currents and wind that caused the buoy to tilt. The different bottom weight application for the prototype and final version spar-buoys is illustrated in Figure 20.

Figure 20. Spar-Buoy Bottom Weight

The different weight types can be observed in Figure 8. The prototype weight (left) and final version weight (right).

The construction of the WSB consisted of drilling holes in both lower and upper end caps to provide an attachment for the 10lb ballast weight and ADAPT sensor nodes respectively. Restraining straps were attached to the upper end caps to ensure that the nodes remained attached to the buoys and would not be lost while conducting operations. The foam ballast was produced by cutting 12-inch by 24-inch rectangular sections that could be wrapped around the PVC pipe and provide the necessary buoyancy at the water line. Galvanized steel eye-bolts were threaded through the pipe at the center of gravity to

provide an anchor attachment point, and 1-inch diameter drainage holes were drilled into the pipe to allow water to easily enter the buoy as it was emplaced and easily exit as the buoy was retrieved. The nylon rope anchor lines and retrieval handles were added to ensure that the buoys did not drift and could be effortlessly retrieved from the side of the boat.

1. Lower End Caps

The lower end caps consisted of a 6-inch inner diameter PVC attachment. It was necessary to attach the lower end caps to the 10-foot pipe with stainless steel rods to eliminate the possibility of the end caps slipping off while deployed. A guide hole was drilled into the side of the end cap, and then broadened to fit the rod. Figure 21 depicts this stage of the construction process.

Figure 21. Lower End Cap with Steel Rod

To enable the 10lb weight plate for ballast to be secured to the lower end cap, four holes were drilled into the base to be aligned with the holes in the 10lb plate. The holes were used to thread a high strength nylon cable tie through them and fasten the plate to

the end cap. Figure 22 depicts the four holes on the base of the lower end cap and how they align with the 10lb plate.

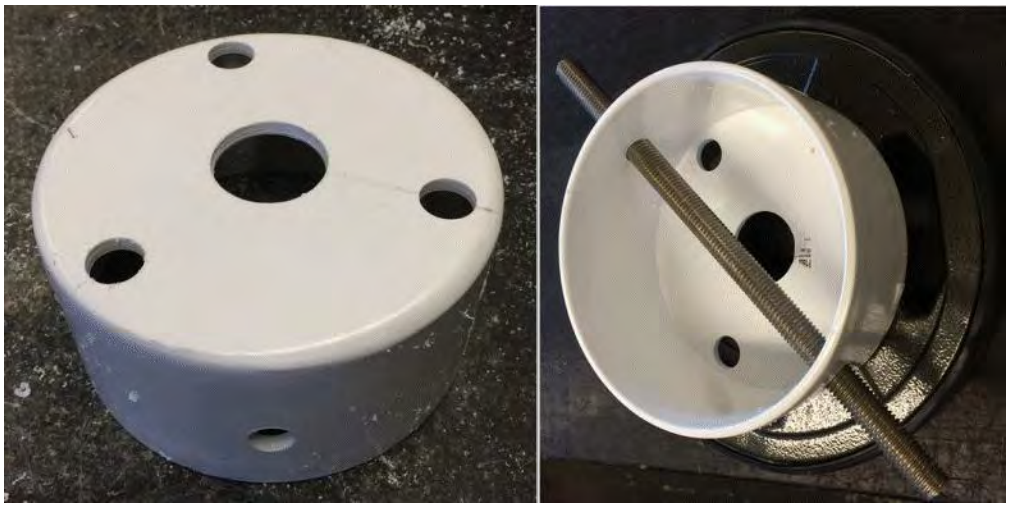

Figure 22. Lower End Cap Holes

Once confirmed that the holes properly align with the end cap the weight was secured using the high strength nylon cable tie as illustrated in Figure 23.

Figure 23. Weight Secured to the Lower End Cap

The lower end cap was completed once the cable ties were cinched and the cap was then attached to the 10-foot PVC pipe. Grease was applied to the threads to facilitate removal of the end cap in the future should it be required.

2. Upper End Caps

The upper end caps also consisted of a 6-inch inner diameter PVC attachment; however, unlike the lower end cap, it was not necessary to attach the upper end caps to the 10-foot pipe with stainless steel rods. To ensure that the upper end caps remained attached to the 10-foot pipes, two screws were fastened through the restraining straps, end caps, and the pipes. Figure 24 displays how the holes to fit the ADAPT nodes were constructed. Without a drill-bit large enough to drill the required 4.95-inch diameter holes, several holes were drilled in each upper end cap and a jigsaw was used to "round out" the required 4.95-inch diameter.

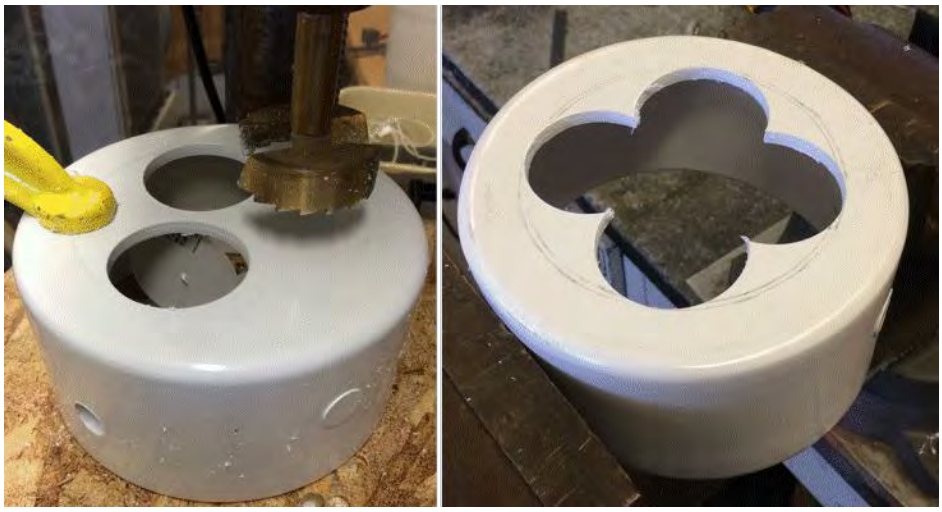

Figure 24. Upper End Cap Construction

Once the 4.95-inch diameter hole was created, the edges were smoothed with the use of a rasp. Figure 25 displays the upper end cap immediately following the use of the jigsaw and then several end caps that have been smoothed by the rasp.

Figure 25. Upper End Cap Hole

Lastly the ADAPT nodes were fitted to ensure that they sat loosely in the hole but that the upper node section (5-inch diameter) would not fall through. Although restraining straps were utilized to secure the nodes to the upper end caps, a rubber strip of tubing was placed around the lower node section so that the fitting would be tight for the node to fit into the upper end cap hole. Figure 26 illustrates the node loosely seated in the hole and tightly seated using the rubber strip.

Figure 26. Upper End Cap with ADAPT Node

3. Restraining Straps

The restraining straps were attached to the upper end caps with screws that not only held them in place but also secured the end caps to the pipes. The straps were adjustable with the use of a metal cinching buckle. When a node was placed in the end cap the straps were tightened to prevent them from falling out during rigorous operations while deployed. Figure 27 depicts the restraining straps attached to the buoy. Of note in the figure is a side view of the rubber seal used in conjunction with the strap to enhance the security of the node and prevent it from detaching.

Figure 27. Restraining Strap

4. Foam Ballast

The foam ballast was produced from 12-inch by 24-inch by 4-inch (12x24x4) thick blocks of polyethylene foam that is frequently used in providing buoyancy for marine equipment. The foam blocks were divided into twelve 2-inch segments laterally across the long side. Once the segments were marked on the foam blocks a band-saw was utilized to cut 3-inch slots into the foam. The purpose of the 3/4 depth was to allow the foam to flex and be appropriately shaped to fit around the PVC pipes while still maintaining its rigidity. Figure 28 illustrates the foam block with the 2-inch segments and the band-saw cutting the 3/4 depth.

Figure 28. Polyethylene Foam Block

The slotted-foam was positioned approximately 1/3 of the distance down from the upper end of the PVC pipes, wrapped around the pipes, and fastened using high strength nylon cable ties. Figure 29 depicts the foam ballast secured around the PVC pipe.

Figure 29. Polyethylene Foam Ballast

The cinching of the cable ties seemed secure enough to prevent the foam from "riding" or "slipping" up the PVC pipes during operations; however, while a minor

concern, it was decided that testing would be performed to confirm or reject any suspicions. During the Phase IV test, the foam did eventually begin to "ride" up the pipes. To mitigate the foam from displacing, wooden dowels were placed through the pipes to hold the foam ballast in place. When the buoy is deployed the foam is designed to be half submerged providing the necessary ballast to maintain the stability of the buoy. Figure 30 illustrates the spar-buoy prototype test, confirming the foam is half-way submerged.

Figure 30. Functioning Foam Ballast

5. Eye-Bolts

The initial design positioned the eye-bolts, which would connect the anchor line to the buoy at the center of the foam ballast, at the water surface (reference Figure 8. Modified Spar-Buoy Design); however, after testing the prototype the eye-bolt was repositioned to a location corresponding to the overall center of gravity of the WSB. Figure 30 includes an initial anchor connecting point located at approximately the center of the foam in close proximity to the water line. It was observed that when the anchor line was "pulled" the buoy would tilt; to avoid tilting reaction the anchor connecting point

would need to be relocated to the buoys overall center of gravity. The method utilized to determine the center of gravity of the WSBs was to balance the buoys (with the ADAPT nodes installed) by a rope. This modification was applied to all follow-on buoys and proved to be a valid design modification. Guide holes were drilled through the PVC pipes and the eye-bolts fitted; the center of gravity for the WSBs was then confirmed by attaching the rope to the eye-bolts. Figure 31 depicts how the center of gravity of the WSB was determined and confirmed.

Figure 31. Center of Gravity

Note the eye-bolt and the rope used to determine and confirm the center of gravity.

The eye-bolts were galvanized steel to provide the strength necessary to maintain the anchor and to prevent the accumulation of rust over a prolonged duration of time. Figure 32 displays the eye-bolt and the eye-bolt with the anchor line connected.

Figure 32. Eye-Bolt

6. Drainage Holes

The drainage holes were an essential contribution to the buoy design. The holes both allowed for the water to enter the buoys to assist with the stability and to exit the buoys as they were retrieved after operations; they also allowed for trapped air to escape. The trapped air would have a negative effect on the stability of the buoy and is necessary for the air pressure inside the buoy to be regulated. During the construction of the prototype buoy a large 3-inch diameter hole was drilled into the lower portion of the PVC pipe; the primary purpose of the 3-inch hole was to provide access for the concrete that had to be poured into the buoy in order to acquire the required 10lbs of ballast weight. The large hole doubled at also providing access for the incoming and exiting of water and air during testing. In addition to the large hole, smaller 1-inch diameter holes were drilled into the sides of the PVC pipe at pseudo-random locations spanning the length of the pipe. The size and quantity of the smaller 1-inch holes was a concern in that they may not be sufficient to transfer the water and air; however, the holes proved to be effective when observed during the Phase IV test. Another potential issue is the tendency of marine life to utilize such holes for "nests." The design may need review after sufficient field deployment to allow for assessment of sea-life intrusion. Figure 33 depicts the large 3-inch hole on the prototype buoy and the smaller 1-inch holes along the span of the buoy.

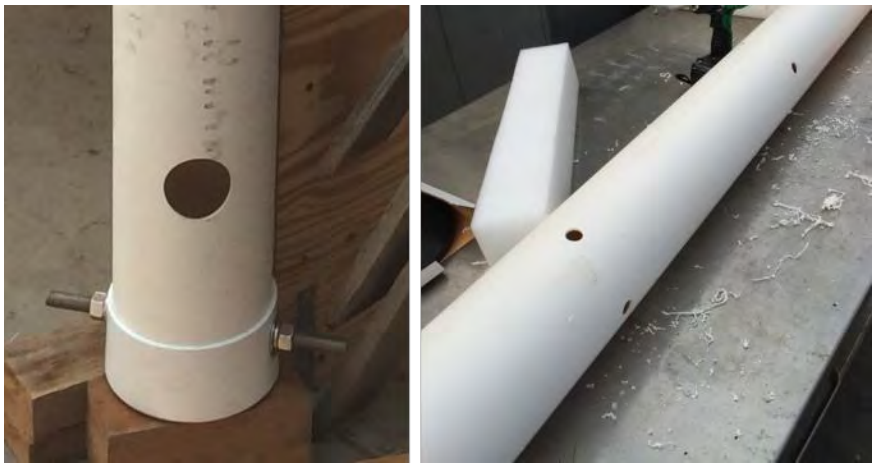

Figure 33. Drainage Holes

The 3-inch hole was only utilized for the prototype and not included in the subsequent buoys.

7. Anchor Lines and Retrieval Handle

The anchors were deemed essential to ensuring that the WSBs maintained their desired topology formation and not drift as a result of ocean currents or wind effects. The anchor consists of a 25-lb plate connected to the buoys via a nylon rope. Since the conduct of the Phase IV test occurred in shallow water at an approximate depth of 15-meters, the length of the anchor lines were set at a length of 25-meters. The purpose of having an anchor line greater than the depth of water is that if the uneven ocean floor extends beyond a depth that is larger than the line, the anchor may pull the buoy beneath the surface. This form of anchor implementation was utilized during testing for this thesis; however, for future testing and for the final implementation of the WSBs a float anchor or para-anchor may be utilized so that the WSB formation maintains its topology. "A sea anchor (also known as a drift anchor, drift sock, para-anchor or boat brake) is a device used to stabilize a boat in heavy weather. Rather than tethering the boat to the seabed, the sea anchor increases the drag through the water and thus acts as a brake." [28]. Sea anchors are currently utilized for boats but may be applied to buoys.

The retrieval handle was effective in not only retrieving the WSBs from the water but also in deploying the buoys. The handle was threaded through two of the 1-inch drainage holes located at the upper portion of the buoy. Manufactured from nylon rope as is the anchor line, the retrieval handle is observed in Figure 34.

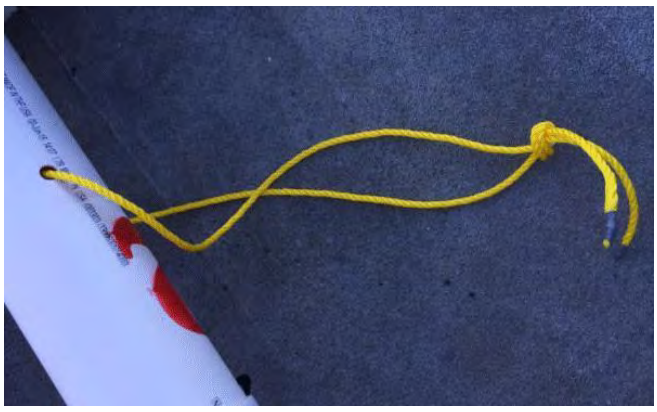

Figure 34. Retrieval Handle

To deploy the WSBs the retrieval handle was utilized to lower the buoys into the water. To retrieve the WSBs a boat hook provided the necessary reach to take hold of the retrieval handle and gain control of the buoy before manually lifting it onto the deck of the vessel. Figure 35 demonstrates the deployment and retrieval of the WSBs.

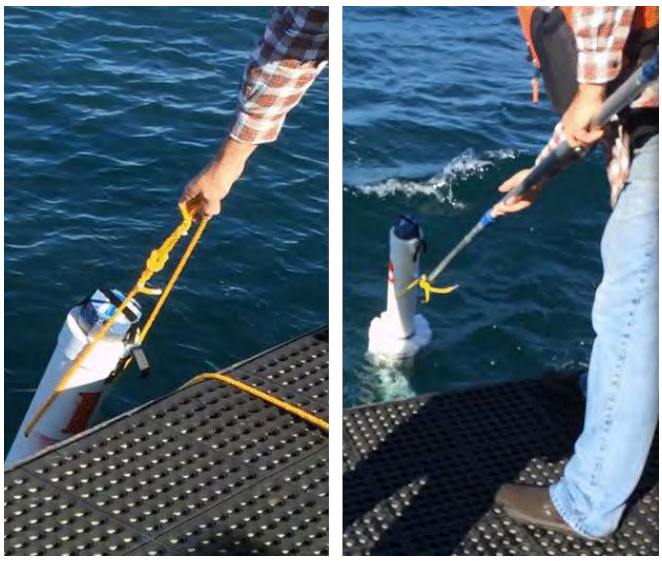

Figure 35. Deployment and Retrieval of a WSB

The left image demonstrates deployment while the right shows retrieval using the boat hook

The anchor, anchor line, and retrieval handle is illustrated in Figure 36.

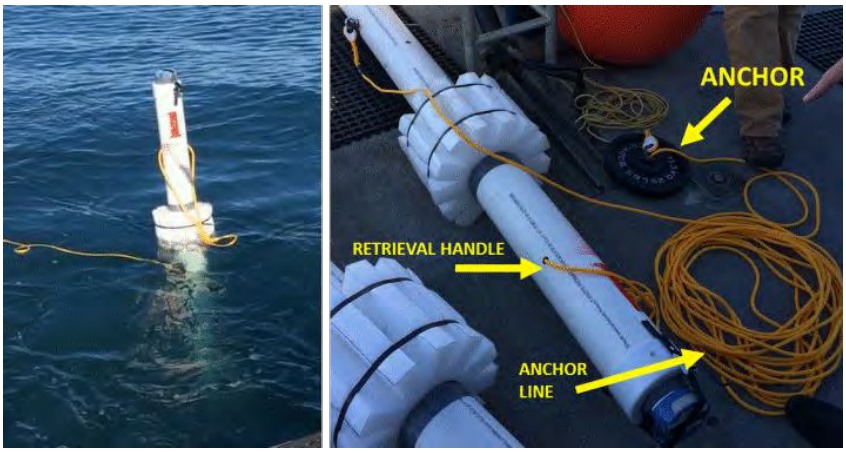

Figure 36. Anchor Line and Retrieval Handle

The key components described above enable the spar-buoy to function as intended and support the ADAPT nodes as they create a wireless network. The design of the WSB provides a lightweight, low-profile, rugged device, which can easily be stored in space restrictive areas aboard naval vessels.

B. MOUNTING OF WSN NODES

A fundamental concern of mounting the ADAPT nodes was that they would not be sufficiently secure and detach while conducting operations. To ensure that the nodes remained attached to the spar-buoys both rubber seating and restraining straps were employed. The PIR sensors remained unobstructed by the straps; although during the Phase IV test they did not function as intended. The restraining straps were adjustable and cinched tight over the nodes once they were installed. Figure 37 illustrates an ADAPT node mounted and ready for deployment.

Figure 37. Mounted WSN Node

After the ADAPT nodes were installed and secured, the nodes could still be turned on and off without having to adjust or remove the rubber seating or restraining straps.

C. WSB NETWORK

The spar-buoy-housed nodes communicated between each other using a 900 MHz radio and, implementing the SIS process, formed a mobile ad hoc network (MANET). Once a MANET is formed nodes used the SAS protocol to share information regarding the location of neighboring nodes, detections of foreign objects, and tracks formed if at least three nodes would detect the same object [4]. The nodes within range of the base station transfer the network data over WiFi using the 802.11n protocol and the data would then be observed by the watch-stander. The operation of the WiFi was possible with the use of a Teletronics International Inc. EZ Platform Access Point/repeater operating at 2.4GHz with a Dell TrueMobile 2300 router for redundancy. The Verizon MiFi hotspot was included should the MSAT be implemented and would need to connect to the server; however, during the conduct of the testing the server was inoperable and the MSAT was not utilized. The watch-stander would view the data on the base station computer, consisting of a 64-bit Intel Core i7 with a 1.80GHz Quad-Core processor running Ubuntu 12.04 LTS.

Prior to performing any operations, the ADAPT nodes must be configured. The nodes were configured using the Lenovo ThinkPad T510 with a dual 2.67 GHz Intel Core i7 CPU and 4 GB RAM running the Ubuntu 12.04.4 LTS 64-bit version operating system. The instructions for imaging the nodes, setting the mission parameters, and checking the status of the nodes are listed in Appendix A. The nodes were physically connected to the ThinkPad with a Universal Serial Bus (USB) cable and adapter plug during configuration. Following the configuration, the nodes were turned off.

In preparation for deployment of the nodes, the Intel base station computer connected to the AP. Once connected, the SIS process was initiated and the nodes activated. A period of five minutes was required before the network could be formed to allow the nodes to acquire a GPS fix and establish their locations [18]. Once established the MANET could report locations, detections, links between nodes, and tracks. During all test phases the WSB network functioned as predicted; however, during the Phase IV test the PIR sensors did not perform as intended and as such no detections or tracks were recorded.

D. SOFTWARE PROGRAM

The Shared Information Space (SIS) process operating on each of the nodes incorporated a peer-to-peer database, which managed the data on the nodes and allowed sharing with neighbors [18]. SIS facilitated the transfer of data between single-hop neighbors. After receiving data the SIS process reevaluated the information and determined if the data was of interest (locations, detections, etc.). If the data was pertinent then the information was forwarded to other neighbors. The many-to-many method of data flow communication is naturally disruption tolerant; it has a circular queue, no message addressing, no routing, and no global knowledge [18].

The applications generated persistent queries for specific data conditions; if the data for which they were "watching" was determined to be pertinent it would get forwarded [18]. SIS combined all the conditions and sent the combined information to its neighbors. The neighbors responded with data that matched any of the conditions and continued to send new data that matched the condition as it was generated. Once data was received SIS notified the appropriate application. During the whole process, the neighbors were conducting the same procedures and were able to form an interlocking set of interest areas [18].

To reduce unnecessary data messages SIS performed various functions [18]. To replace data messages, for example the node location changes, the data was replaced in the packet on the output queue and then restored to all the neighbors. When the data remained unchanged it expired after 60-seconds and the packet was removed from the output queue. If the same incoming data message was received (same data record was on the output queue), then the duplicate source data was "dequeued." Should a neighbor disconnect, the index in all queued records was reduced and the record was "dequeued." When a neighbor reconnected, its index was added to all queued records [18].

E. TESTING

The testing was vital to confirming the legitimacy of the proposed application of WSBs for perimeter security of naval vessels and seabases. Testing was conducted in an

incremental manner by confirming capability, functionality, and, finally, feasibility. The test results provided validation, insight into modification, and ideas for future testing.

1. Summary of Action

To prove the concept of a WSB system for the protection of naval vessels, a wireless network was required to be implemented on the ocean surface and be tested to prove its efficacy. To apply this concept, the pre-existing ADAPT nodes were utilized. Before testing the WSBs, confirmation was required that the nodes would function on stable, dry terrain; once the nodes were validated they could be mounted on buoys and tested on the water surface. The test plan was divided into four phases to prove the concept. Test phases I and II were conducted on dry land in order to validate range, network topology, and the wireless network. Test phases III and IV were conducted on the water surface to confirm that the modified spar-buoys functioned as they were designed and to test the MANET on the ocean surface. Future testing ideas were identified for follow-on research.

The purpose of the tests conducted for this thesis were to determine if the ADAPT wireless sensor nodes could be mounted on buoys to form a WSN in order to communicate incoming small vessel surface threats. The tests were conducted to test for range, topology, networking, functionality of the buoys, and finally whether the nodes would form a network and function correctly on the ocean surface.

Specifications acquired from the Institute of Electrical and Electronics Engineers (IEEE) suggest that the 802.11n protocol should provide effective data transfer for a range of 70 meters from the indoor router and an outdoor range of up to 250 meters [29]. Based on the provided information, the distances for the required topology was estimated to be a range of no more than a 250-meter radius from the vessel; however, the range would be tested at significantly shorter distances and incrementally increased to establish a suitable and reliable distance between the nodes and the base station. The proposed final topology of WSBs is depicted in Figure 2.

The initial test, Phase I: Dry Land Range Test, was established in order to determine the maximum effective range and reliable range that the current ADAPT sensor nodes, using the WiFi 802.11n protocol, are capable of effecting. The setting for

the test was a flat unobstructed surface with direct line of sight. The test also included adding multiple nodes in opposite directions to determine if network interference would affect the range.

Following the completion of the Phase I test, the proposed topology could be tested and the secondary test, Phase II: Dry Land Functional Test, could be conducted. This phase was divided into two parts. Part A utilized eight nodes and a base station cluster in a compressed topology with a radius of approximately 40 meters. This test was conducted to determine what might be expected from the implementation of the proposed topology when the nodes are mounted on the buoys. It is important to note the test was conducted on dry, stable land that did not take into account ocean effects. As in Phase I, the setting for the test was a flat unobstructed, open surface with direct line of sight between all the nodes and the base station cluster. A consideration during the Phase II Part A test was that the nodes would not be in motion as they were not on the dynamic water surface but rather fixed on dry land. To simulate the vertical motion that a node may experience, a single node was moved in an up and down gesture. Another issue with the Phase II Part A test plan was the absence of swells that would undoubtedly be encountered while on the ocean; such swells may inadvertently trip the PIR sensors on the nodes. However, the swells could not be simulated during the Phase II test.

At the completion of the Phase II, Part A test, Phase II Part B was conducted. This test was designed to test and confirm the wireless network as it performs on dry, solid land. The topology of the network tested was intended to be similar to the topology that would be utilized for the Phase IV test, which was to be conducted with the spar-buoys on the ocean surface. The Phase II Part B test would verify the functionality of the network where normally a node beyond the maximum 250-meter range for 802.11n would relay its information via neighboring nodes back to the base station. Several conditions would need to be tested, to include locations of nodes throughout the network, PIR detections, and node links.

Following the completion of the Phase II tests, the modified spar-buoy design was tested. The third test, Phase III: Spar-Buoy Test, was conducted to determine the buoyancy and balance of the spar-buoy. In addition to the buoy functionality, an ADAPT node was mounted on the spar-buoy to test the WSB configuration and ensure that the

node communicated with the base station as intended. The setting for the test was a relatively calm body of water that included a water depth sufficient enough to provide unobstructed interference with the lower end of the buoy against the floor. A concern during this phase was if the motion of the water surface would inadvertently trip the PIR sensor on the node. In addition to functionality tests, another purpose of the Phase III test was to determine whether any modifications may be required to the spar-buoy before conducting Phase IV testing.

Following the completion of the Phase III test, modifications to the design were identified and implemented. The fourth and final test performed for this thesis work was the Phase IV: Ocean Concept Test, which was conducted on the ocean surface. The purpose of this test was to determine if the ADAPT wireless sensor nodes could be mounted on buoys to form a WSN, which would facilitate threat warnings by more capable sensors as part of future work. Although not a requirement, the PIR sensors would also be tested to assess the likelihood of interference by ocean swells with network operation. The setting for the test was to be a large body of water that included a water depth sufficient enough to provide unobstructed interference with the lower end of the buoy against the ocean floor, and an environment where line of sight was achievable. A consideration during this phase was the accurate deployment of the WSBs at the specified ranges. Another concern was that the ADAPT nodes, although water-resistant, may be susceptible to moisture from the ocean which would cause the nodes to malfunction.

2. Phase I Testing

Phase I were conducted at the beach in Del Monte, Monterey, California where mostly clear line of sight between the nodes and the base station could be maintained. During the tests, some sand dunes were utilized as obstacles preventing clear line of sight; this had a minimal impact on the data that was collected at the ranges tested. Multiple nodes were introduced to the test in opposite directions from the base station to determine if network interference would affect the range at which the nodes were able to function. Figure 38 illustrates the base station and wireless Access Point (AP) in its operational configuration.

Figure 38. Base Station and Access Point

The distances used to test the ranges of the nodes are depicted in Table 2. An additional node was added to the network to test if it affected the communication of the primary node (CD51). Note that the identifier used for each node is derived from the node serial number. The comments section represents the quality of the reports received by the base station. During some occasions the nodes responded with a delay in reporting and other times nodes did not report a position. Each node's onboard GPS locations were validated utilizing a handheld Garmin GPS.

Table 2. Single Node Range Data

NODE ID	DIST(m)	LOCATION (GPS)	COMMENTS
Base Station	N/A	N/A	N/A
CD51	0	36.602733 -121.873659	Delayed Reporting
	75	36.603112 -121.873008	Good Detection
	100	36.603328 -121.872756	Good Detection
	110	36.603380 -121.872691	Delayed Reporting
	130	36.603488 -121.872517	Good Detection
	140	36.603508 -121.872398	Delayed Reporting

Table 2 depicts the range data for a single node.

The distance between the node and base station was 75 meters. Figure 39 illustrates the map overlay for the single node range test.

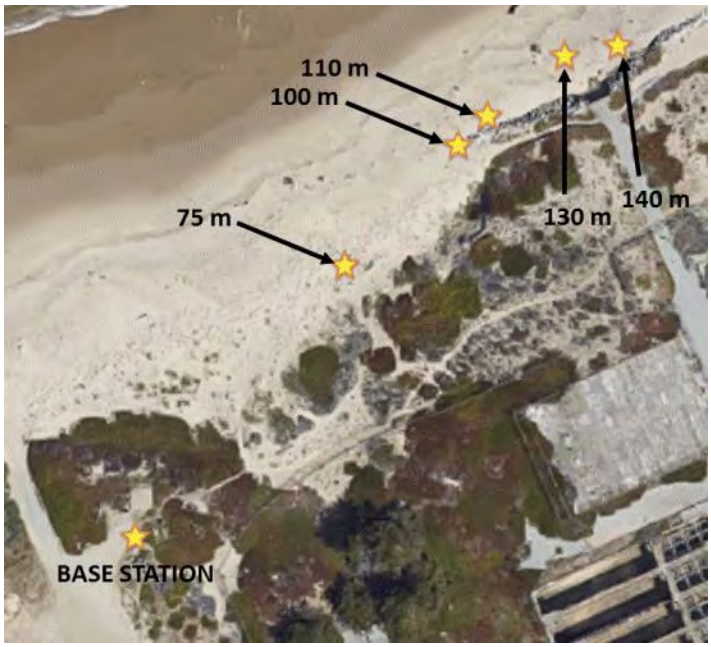

Figure 39. Map Overlay—Single-Node Test

The positions of CD51 during the single node tests. Adapted from: Google maps, Imagery Google map data 2015. [Online]. Available: https://www.google.com/maps/ Accessed Dec. 2, 2015.

Node CD51, the node utilized to conduct the single node range tests provided unusual data. Initially, the node was placed beside the base station at a range of less than one meter; the node did report its position, however, it was delayed by approximately 10 seconds. The nodes require approximately five minutes to acquire a GPS position once activated; CD51 was tested at the five-minute mark but may not yet have acquired its GPS position before the request for its location was issued. Once acquired, CD51 did report its location. At 110 and 140 meters the reporting by CD51 was also delayed; this may have been due to noise, or a faulty node. The node did not acquire a location beyond 140 meters. A screen shot of the data produced with the SIS process is depicted in Figure 40. It shows that CD51 acquired a successful detection.

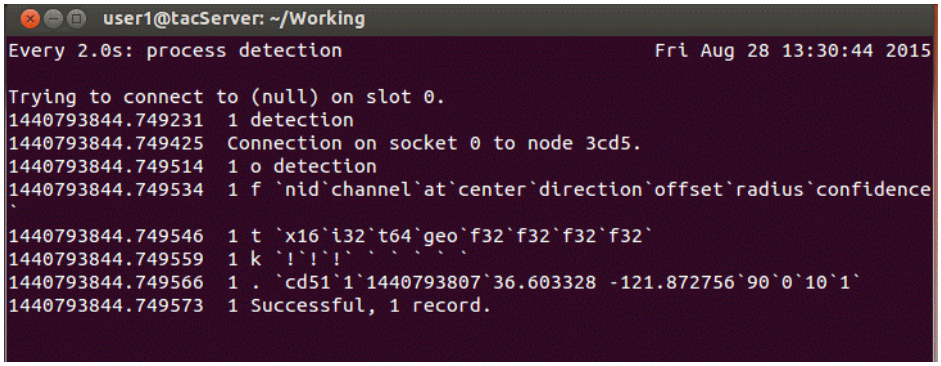

Figure 40. Single Node Detection Record at 75 Meters

The data in Figure 39 displays date and time that the testing occurred and that every two seconds an update was produced. The first four lines of values represent the base station computer as is indicative of the node identification "3cd5." The following four lines of values represent the ADAPT node during the test "cd51'.

Following the single node range test, CD51 was relocated to the opposite side of the base station at a distance of approximately 60 meters, and an additional node (A9DB) was introduced to the network. A9DB was positioned approximately 100 meters from the Base Station on the opposite side from CD51. When A9DB joined the network it had a delayed response time for submitting the report of its location and CD51 did not report its position. These results are depicted in Table 3.

Table 3. Multi Node Range Data

NODE ID	DIST(m)	LOCATION (GPS)	COMMENTS
Base Station	N/A	N/A	N/A
CD51	60	36.602716 -121.874132	No Reporting
A9DB	100	36.603328 -121.872756	Delayed Reporting

The multi-node range test yielded unsatisfactory results even though both nodes were positioned within 100-meters of the base station. The map overlay is observed in Figure 41.

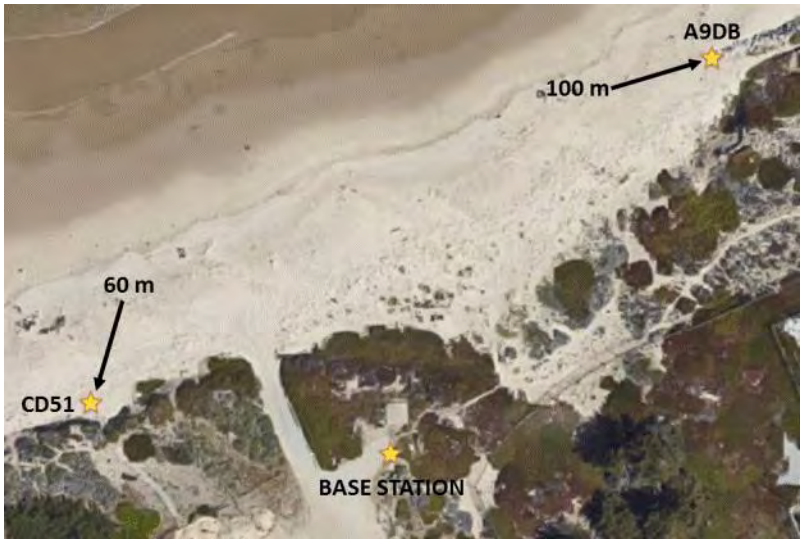

Figure 41. Map Overlay—Multi-Node Test

The positions of CD51 and A9DB during the multi node test. Adapted from: Google maps, Imagery Google map data 2015. [Online]. Available: https://www.google.com /maps/ Accessed Dec. 2, 2015.

Although the objective of the Phase I test was met, which was to test the range of a single node, the overall results were disconcerting. The unsatisfactory results could be attributed to numerous issues, such as noise caused by other devices in the area operating on the 2.4 GHz frequency; this would account for the disruptions and the delays. Other issues may be that the nodes themselves were faulty, or that a fault in the developmental software may exist. Additional detailed testing would need to be conducted to determine the exact issue.

3. Phase II Testing

The Phase II dry land functional test was divided into two parts, as noted. Part A utilized eight nodes and the base station cluster in a compressed topology similar to the topology that will be implemented during the employment of the WSB system. The perimeter was reduced to a radius of approximately 40 meters whereas the final implementation may extend to a radius in the range of over 100 meters. The purpose of this test was to determine what may be expected from the implementation of the proposed topology for when the nodes are mounted on the buoys. The test was conducted on land eliminating any ocean effects, such as propagation over water or dynamic motion due to

ocean swell. Part B also made use of eight nodes; however, during this part they were deployed in a column topology with the intent of confirming that the MANET functioned correctly and nodes beyond the WiFi range relayed information back to the base station. Part B tested whether the nodes reported both locations and detections. Results of the test follow.

a. Part A Testing

The eight nodes utilized for the Part A test were positioned in a perimeter around the base station cluster, in a "spoke-and-wheel" fashion where every node could communicate with the base station cluster directly. Table 4 lists the nodes, their locations, and comments regarding their detection status.

Table 4. Compressed Topology Test

NODE ID	NODE GPS	COMMENTS
Base Station	N/A	N/A
100C	36.597495 -121.869563	Detection
DB72	36.597411 -121.869816	Detection
41F1	36.597468 -121.870093	Detection
512A	36.597587 -121.870173	Detection
FDAC	36.597833 -121.870195	Detection
C588	36.598055 -121.869928	Detection
BO34	36.597953 -121.869605	Detection
32B4	36.597771 -121.869589	Detection

The data in Table 4 consists of the base station and eight ADAPT nodes. The nodes were oriented in a topology to represent the final proposed configuration.

The detection testing was implemented by running alongside each of the nodes and determining if the PIR sensors were triggered. Each of the nodes reported the detections, which was observed on the base station with the SIS process. The topology during Phase II Part A is depicted in Figure 42.

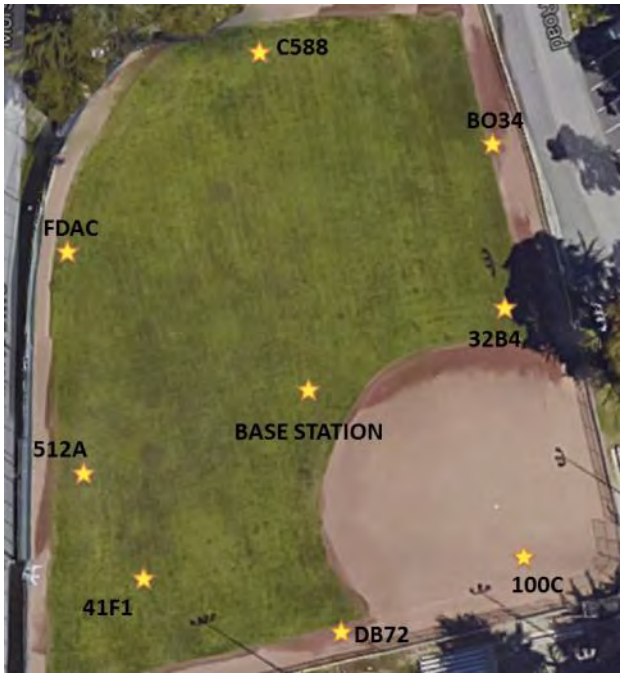

Figure 42. Compressed Topology

The compressed topology with an approximate distance of 40-meters between the nodes and base station. Adapted from: Google maps, Imagery Google map data 2015. [Online]. Available: https://www.google.com/maps/ Accessed Dec. 2, 2015.

A simulated buoy-in-motion test, as described above, mimicked the expected movement of the node while running the SIS process. Table 5 depicts the captured location data from the node as it transmitted while moving.

Table 5. Simulated Buoy Test

NODE ID	NODE GPS	COMMENTS
Base Station	N/A	N/A
512A	36.597597 -121.870168	Detection
	36.597624 -121.870170	Detection
	36.597651 -121.870176	Detection
	36.597702 -121.870153	Detection

Table 5 illustrates the motion test which suggests that the node communicated its position while in motion. Theoretically these results are a valuable milestone for follow-on testing in Phases III and IV.

All the nodes during the Phase II, Part A test functioned as intended providing satisfactory results. After the nodes were emplaced, and the five minute GPS acquisition window for each of the nodes had concluded, each of the node locations were verified with the SIS process. The SIS location data is presented in Figure 43.

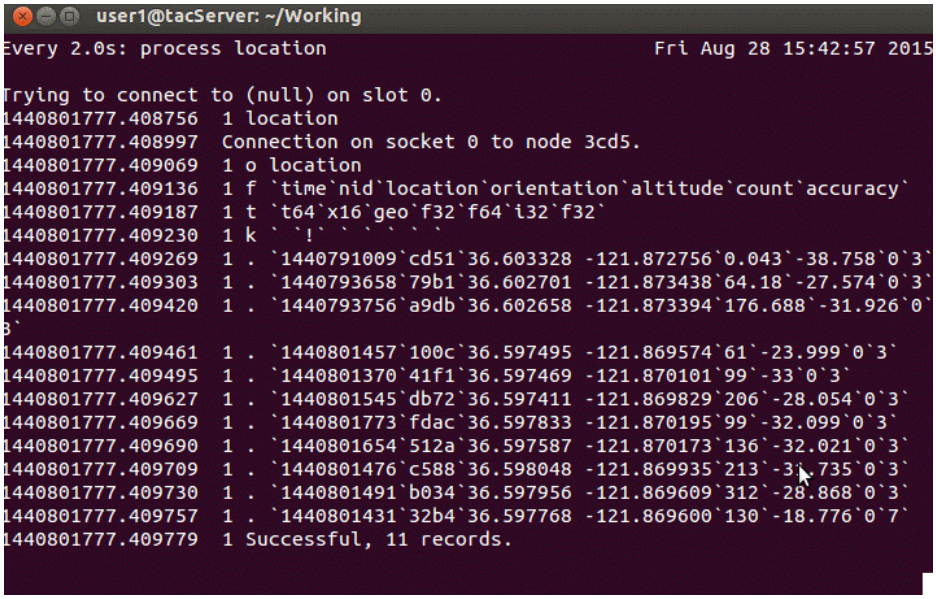

Figure 43. Phase II Part A: SIS Location Data

The 11 records for location include the eight nodes used in the Phase II Part A test and the three nodes that were activate during the Phase I test; a clear indication that a software discrepancy in the developmental SIS process may exist.

To ensure that the location data provided by the SIS process was accurate, a hand-held Garmin GPS was utilized to validate the reports. Of special interest in the SIS report, in Figure 43, was that the data of the locations for the nodes from Phase I remained. When referencing Figure 39. Single Node Detection Record at 75 meters and comparing the GPS coordinate location for node CD51 to its reported location in Figure 43. Phase II Part A: SIS Location Data, the locations were the same. Further analysis of the data revealed that the Phase II Part A testing location was well beyond the range of the location reported by CD51; this node would be implementing the 802.11n protocol for communication but the range was approximately 680 meters line-of-sight with obstacles in between the nodes. The maximum range for 802.11n, with no obstacles, is only

estimated to be 250 meters [29]. Another observation was the time elapsed between Phase I and Phase II Part A tests. The location for CD51 during Phase I generated the SIS report at 13:30:34 and the location for CD51 during Phase II Part A was generated at 15:42:57; the difference in time between reports was 2:12:23 (over two hours). The significance of the time difference is that the SIS process is designed to clear the output queue after 60 seconds if the data remains unchanged. Lastly, node CD51 was turned off and inactive during the time Phase II Part A testing was being conducted. The evidence suggests that the developmental SIS process may be faulty.

b. Part B Testing

The eight nodes utilized for the Part B test were positioned in a linear topology to confirm that nodes extending beyond the maximum 802.11n communication distance would relay their information to their neighbors and, ultimately, to the base station. For Phase II Part B the Sitmap, a graphical map produced by ADAPT, was implemented. Sitmap was only utilized during this test since it merely covered a small area dedicated to this portion of the map. Figure 44 illustrates the deployment of the ADAPT nodes as portrayed by Sitmap.

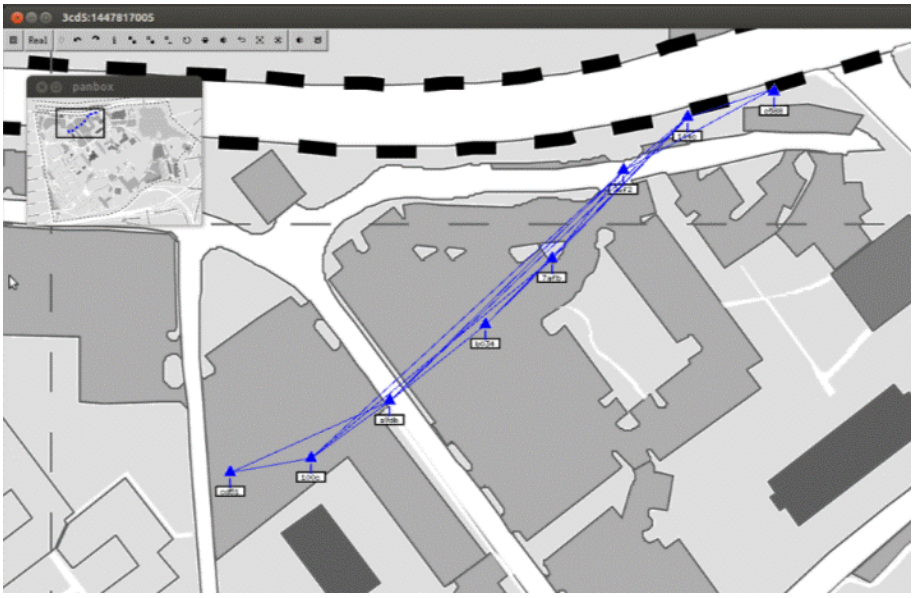

Figure 44. Phase II Part B Initial Topology

In the figure, the solid lines between the nodes represent the links created as part of the wireless network. Sitmap displays not only the map area, but also the location of the nodes and the links between them. The locations for each of the nodes are represented in Table 6.

Table 6. Phase II Part B Linear Topology

NODE ID	NODE GPS	COMMENTS
Base Station	N/A	N/A
CD51	36.598706 -121.876346	Successful Link
100C	36.598743 -121.876054	Successful Link
A9DB	36.598893 -121.875768	Successful Link
BO34	36.599094 -121.875421	Successful Link
7AFB	36.599266 -121.875181	Successful Link
26F2	36.599497 -121.874921	Successful Link
144C	36.599636 -121.874690	Successful Link
C588	36.599704 -121.874376	Successful Link

The distance from the base station to the furthest node (C588) was approximately 230 meters, with obstacles in-between, which is at the outer limits of the range for 802.11n. The SIS process from the base station, depicting the location reports of the eight nodes as they reported directly to the base station as intended, is represented in Figure 45.

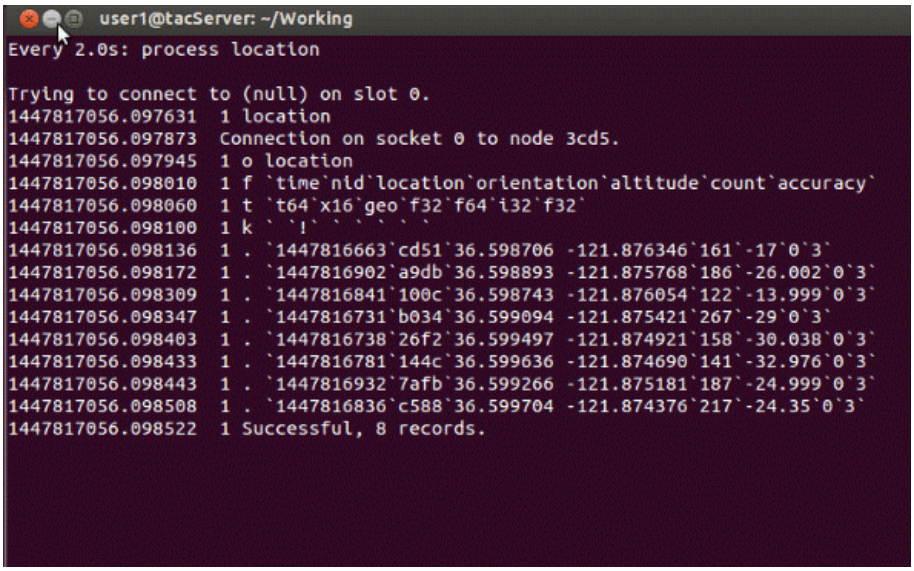

Figure 45. Phase II Part B: SIS Process Initial Locations

After successfully acquiring data representing all eight node locations and their links, node-6 (26F2) was relocated to the furthest position to observe the behavior of the network and confirm that communication with the base station was still possible at the increased range. Figure 46 depicts the change to the topology.

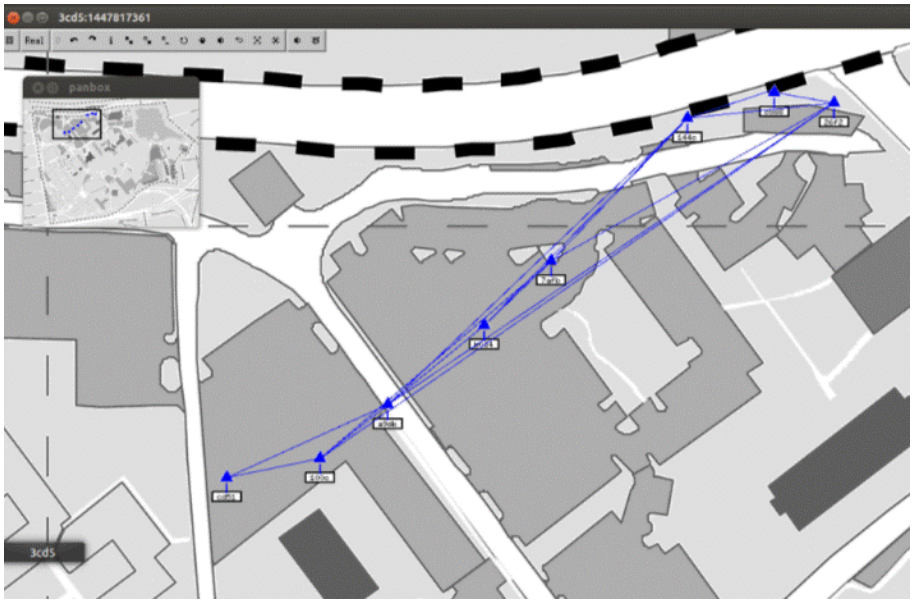

Figure 46. Phase II Part B: Modified Topology

Node-6 (26F2) was relocated to a position located at 36.599677 -121.874161, approximately 250-meters from the base station with obstacles in-between. Communication from node-6 with the base station directly would have been highly unlikely at the maximum range for 802.11n, yet the records of node-6 were still displayed by SIS on the base station. Analyzing the links represented by the Sitmap in Figure 46, node-6 (26F2) established a connection with node-2 (100C) directly using the 900 MHz ground radio and SAS protocol. Node-6 did not have an established link with node-1 (CD51) which was furthest from node-6, which suggests that node-6 was sharing its information with other nodes in the network, which were relaying node-6's information to the base station.

The PIR sensors were tested and the results represented on the Sitmap. As the nodes were retrieved, detections were still being reported by SIS for a period of time exceeding 60 seconds, which suggests "shadow" data reports. Figure 47 illustrates the delayed detection reporting by the SIS process during the Phase II Part B test.

Figure 47. Phase II Part B: Delayed Detection Reporting

Note the circular shapes representing detections and that the two in the upper left corner have no node present at its epicenter.

At the conclusion of the Phase II Part B test it was determined that the ADAPT nodes were able to successfully establish a MANET. Both the 802.11n and the 900 MHz radios functioned effectively, allowing communication between nodes and to the base station. The only discrepancy during the test was the delayed reporting of the detections by the SIS process. The same topology utilized during Phase II Part B would be implemented in Phase IV to test the network as the ADAPT nodes were mounted on buoys and deployed in an ocean environment.

4. Phase III Testing

Phase III: Spar-buoy test was conducted to determine the buoyancy and balance of the spar-buoys and to determine node communication on the water. The initial test of Phase III confirmed that the modified spar-buoy functioned as intended. The buoy was deployed in a harbor environment where control of the device could be easily maintained. It was primarily tested without the ADAPT node attached; this was such that in the event the spar-buoy malfunctioned the sensor node would not be lost. The concern that the foam ballast might "slip" was not realized as the high strength ties held the foam in position. The initial spar-buoy test is pictured in Figure 48.

Figure 48. Spar-Buoy Prototype Test

After confirming the functionality of the spar-buoy, the ADAPT sensor node was attached. The buoy maintained a steady balance and provided the necessary buoyancy to perform further testing. The SIS process was initiated and the location of the WSB was reported to the base station. Following the location report the PIR sensor was tested; however, the detections were reported sporadically and unreliably. The secondary spar-buoy test to include the ADAPT node attached is pictured in Figure 49.

Figure 49. Spar-Buoy Prototype Test with The ADAPT Node

Note the location of the anchor connection point situated at the water-line; this would be modified with the future models.

The inconsistent detection reporting observed during the testing was attributed to either the dynamic nature of the water or attributed to the speculated cause of discrepancies observed in both test phases I and II. The water, constantly in motion, may have "triggered" the PIR sensor resulting in false-positive readings. When the PIR sensor is "triggered" it reports the detection and after 60 seconds resets [18]; however, if the sensor is constantly being "tripped" due to the movement and temperature variants between the water and the air, the sensor may not have the ability to adequately recover in order to reset, and thus produce inconsistent data.

At the conclusion of the Phase III test two deficiencies were identified with the spar-buoy prototype design, both of which were described in the design process in Chapter III. The most significant modification required was to the anchor connection point location situated at the water-line. When the buoy was guided with the anchor line it was observed to tilt; the tilting was due to a moment arm created by the offset center of gravity. This could prove detrimental to the functionality of the ADAPT nodes when deployed in more turbulent ocean conditions where the wind and ocean currents would impact the buoy motion. To remedy the tilting, the anchor connection point would have to be located at the spar-buoys center of gravity.

Another modification suggested for application to the buoys was to replace the concrete ballast weight located at the lower portion of the buoy with a 10lb weight-plate. This would enable ease of manufacture and increase the precision of the ballast weight utilized. Using an "attachable" weight plate would also create versatility for the spar-buoy; should a heavier node or instrument be required to be mounted on the upper portion of the buoy, the ballast weight would also need to be increased. An attachable weight plate would be interchangeable and could be refitted rapidly without significant effort or associated costs.

5. Phase IV Testing

Phase IV: Ocean Concept Test was executed to determine if the ADAPT wireless sensor nodes could be mounted on buoys to form a WSN to communicate the intrusion by incoming small vessel surface threats. After applying the suggested modifications to the spar-buoys following the Phase III test, the WSBs were deployed in an ocean environment. The overall system configuration remained unchanged; however, the base station was situated aboard a vessel and the WSBs were transported by the same vessel and deployed from the aft of the boat. The proven topology conducted during the Phase II Part B test was implemented in this phase, which dispersed the nodes in a linear pattern. The distances between the nodes were established at approximately 40 meters and after confirming that the network functioned as intended were incrementally increased according to the test plan (reference Appendix B. Phase IV test Plan). The location and link processes were reported to the base station cluster aboard the vessel and is represented in Figure 50.

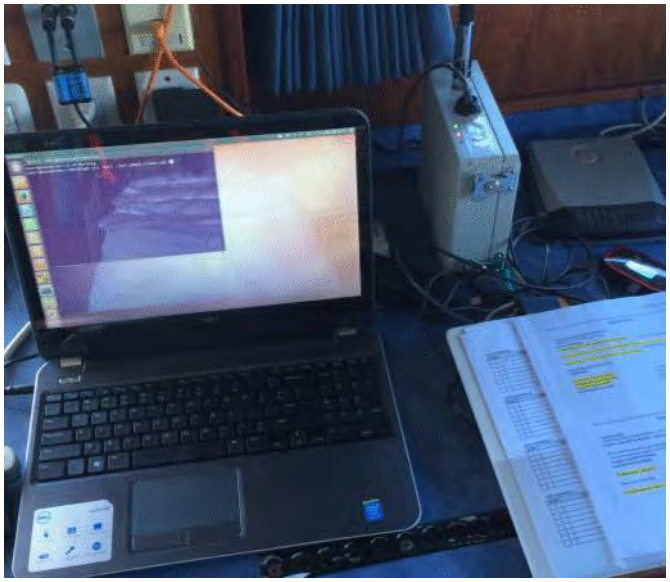

Figure 50. Phase IV Base Station

The WSBs were initially deployed according to the test plan. However, the test was modified due to the difficulty of accurately positioning the WSBs and the impending weather conditions on test day. The difficulty in positioning the WSBs was attributed to both the drift of the buoys after the anchor had been released and maneuvering the boat to within a reasonable amount of accuracy to the required location. Since the ocean floor was uneven the distance from the anchor to the surface of the water would vary as the buoy drifted with the ocean current. These factors caused minor deviations from the intended positions. A view from the boat deck depicted in Figure 51 illustrates the difference in intervals between WSBs as a result of the uneven ocean floor and the difficulty of maneuvering the boat to the precise location for release of the buoys. Regardless of the effort to emplace the WSBs in their precise locations for testing, the boat driver and crew were able to disperse the buoys with a sufficient accuracy to fulfil the intent of the testing goals.

Figure 51. WSB Dispersion

The primary test was initiated as planned with the WSBs, except that the nodes were dispersed at approximately 40 meters intervals, as noted. It was decided that this dispersion distance would suffice for the purpose of the initial test. The WSBs, to include their attached ADAPT nodes, were numbered as indicated in Table 7. The table includes the GPS location of the WSBs during the initial test at the 40-meter dispersion and includes whether the location, link information, and any detections were reported by the SIS process.

Table 7. Phase IV Test: 40 Meter Dispersion

WSB NUM	NODE ID	NODE GPS	LOCAT	LINK	DETECT
N/A	Base Station	N/A	N/A	N/A	N/A
1	CD51	36.608293 -121.875753	YES	YES	NO
2	100C	36.608304 -121.875276	YES	YES	NO
3	A9DB	36.608365 -121.875116	YES	YES	NO
4	BO34	36.608564 -121.874738	YES	YES	NO
5	7AFB	36.608628 -121.874367	YES	YES	NO
6	26F2	36.608988 -121.873909	YES	YES	NO
7	144C	36.609168 -121.873619	YES	YES	NO
8	C588	36.609294 -121.873275	YES	YES	NO

The SIS process reported the locations for each of the nodes and all the links between nodes within the network. However, no reports of detections were received. After analyzing the log files of the nodes it was determined that detections did in fact occur, but due to the high regularity of detections, likely attributed to the motion of the water, the SIS process would constantly dequeue the data messages before forwarding them to a neighbor or the base station. In other words, the neighbor received an initial detection; however, before forwarding the information to other neighbors it received another detection. The second detection required it be checked against others in the queue for duplication. Since it occurred immediately following the first, the second detection was viewed as the same incoming data message. The function checked the output queue and determined that the second message was a duplicate and dequeued the second message.

A third detection occurred and was again viewed as the same data message and also dequeued. This pattern continued for 60 seconds as the initial detection data message was unable to leave the queue due to checking as new detections continued to be received. After 60 seconds, the data was determined to have remained unchanged and expired. The packet was then removed from the output queue and the process continued as a new first detection occurred. In short, detections occurred too frequntly for the nodes to process the data and forward the message without risking substantial duplicate or false-positive reports.

Although no detections were reported to the base station, the link data was presented. The link data displayed by the SIS process is illustrated in Figure 52.

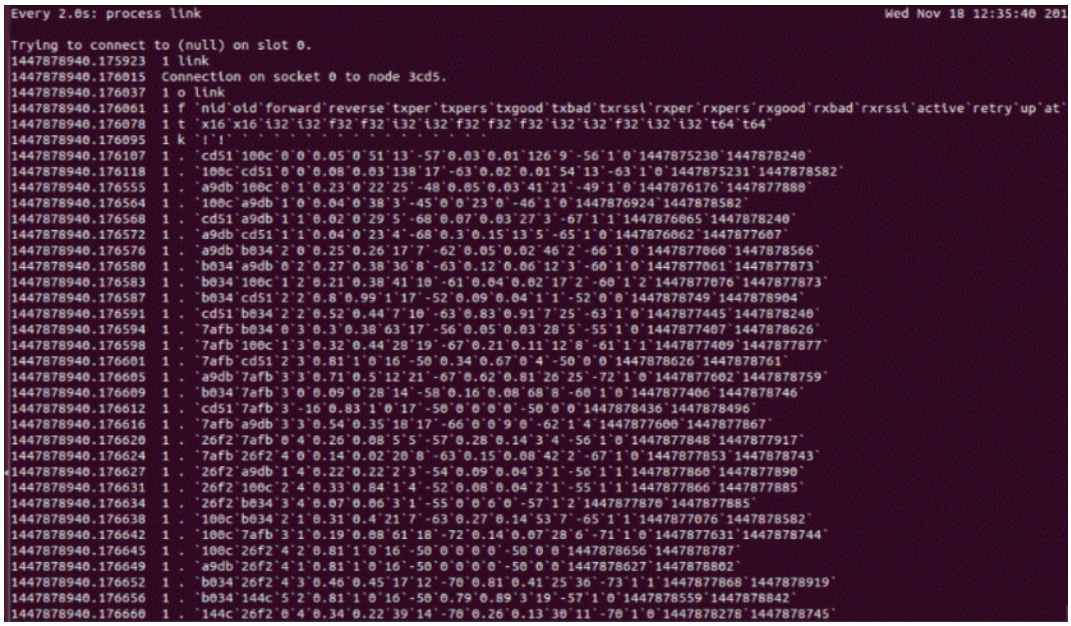

Figure 52. Link Data at 30 Meter Dispersion Test

From the data in Figure 52 it can be observed that CD51, located on WSB-1, has created a link with at least four neighbors. The topology was linear with an average dispersion between buoys of 40 meters. When testing for WSB locations the base station aboard the vessel was located approximately 50 meters beyond WSB-1. The furthest buoy (WSB-8) was located approximately 300 meters from the vessel. Dispite a distance beyond the maximum for 802.11n, a record of the location for WSB-8 was reported to the base station by using the 900 MHz radio to forward data between neighbors. A Google map image during the initial test is superimposed with the WSBs as illustrated in Figure 53.

Figure 53. Map (Phase IV 40-Meter Test)

The nodes are employed in a linear topology formation. Adapted from: Google maps, Imagery Google map data 2015. [Online]. Available: https://www.google.com/maps/ Accessed Dec. 2, 2015.

At the completion of the 30 meter test, the Test Plan required WSBs 2, 4, 6, and 8 to be relocated; the relocation would increase the dispersion between nodes to 60 meters. The difficulty of deploying the buoys accurately and the 40 meter dispersion from the first test resulted in the secondary test producing a dispersion distance of approximately 90 meters between WSBs. The WSB locations and SIS reporting confirmations following the secondary test are depicted in Table 8.

Table 8. Phase IV Test: 90 Meter Dispersion

WSB NUM	NODE ID	NODE GPS	LOCAT	LINK	DETECT
N/A	Base Station	N/A	N/A	N/A	N/A
1	CD51	36.608293 -121.875753	YES	YES	NO
2	100C	36.608304 -121.875276	YES	YES	NO
3	A9DB	36.608316 -121.875145	YES	YES	NO
4	BO34	36.608451 -121.873940	YES	YES	NO
5	7AFB	36.608628 -121.874367	YES	YES	NO
6	26F2	36.610403 -121.872618	YES	YES	NO
7	144C	36.609121 -121.873551	YES	YES	NO
8	C588	36.609584 -121.873009	YES	YES	NO

The end-to-end distance of the network during the second test was approximately 450 meters. However, it is important to note that the location data for nodes 2 and 4 are incorrect; a delay in the SIS process likely presented an outdated report for the location for nodes 2 and 4 while in transit, which was eventually resolved. A Google map image during the secondary test is superimposed with the WSBs as illustrated in Figure 54.

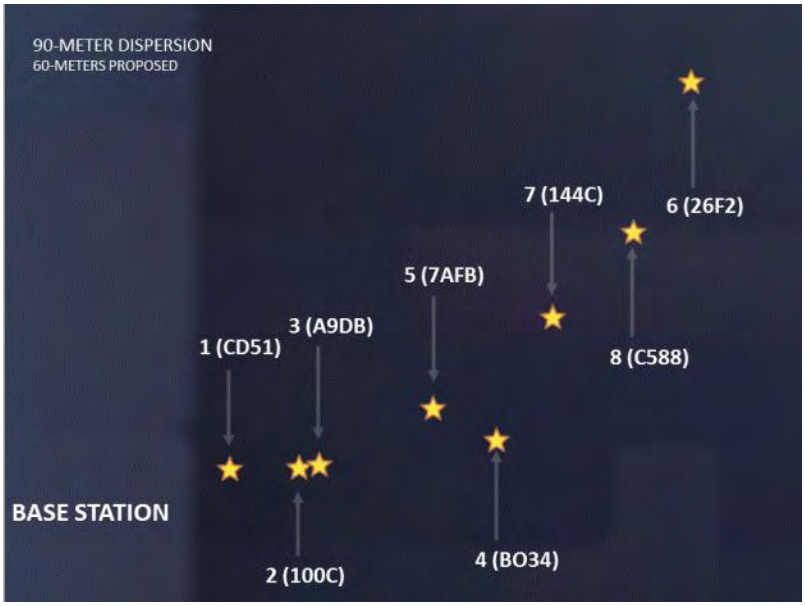

Figure 54. Map (Phase IV 60-Meter Test)

Note the incorrect reported positions of nodes 2 and 4. Adapted from: Google maps, Imagery Google map data 2015. [Online]. Available: https://www.google.com/maps/ Accessed Dec. 2, 2015.

Impending inclement weather caused the remainder of the Phase IV Test Plan to be modified. The distance of WSB-6 from WSB-4 was increased by an additional 120 meters following the second test, increasing the distance between the two WSBs to more than 200 meters. The vessel then relocated to a position approximately 90 meters from WSB-1. The total range from the vessel to WSB-6 was approximately 550 meters. After the relocation of both the vessel and WSB-6, the SIS process displayed a link between WSB-6 and WSB-7; the distance between these two nodes exceeded 250 meters. The result of the link suggests that the 900 MHz radio may be capable of maintaining a connection at this extended range.

The remaining time for testing was limited and it was decided to conduct one last test. WSB-6 again was relocated to extend the distance from WSB-4 by an additional 120 meters. Running the SIS location process yielded that the position of WSB-6 had not been altered and displayed its last known position approximately 200 meters from WSB-4. The error in reporting may be attributed to a software problem with SIS.

During the later stages of testing the foam ballast on several of the buoys shifted upwards toward the sensor nodes, confirming the risk that was anticipated during the buoy design effort. The foam shifted as the foam loosened during operation in the turbulent ocean environment. To resolve the foam slippage a wooden dowel was placed through the PVC pipe as well as the foam and secured with duct tape as proposed in the design phase. The modification proved effective, as the foam did not experience any further slippage for the remainder of the tests.

At the conclusion of testing the linear topology, the WSBs were collected. WSB-7 was the first buoy to be retrieved and upon retrieval the node was removed from the buoy and turned off. Following the elimination of WSB-7 from the network, a test to determine the location of the remaining WSBs was conducted. The data that the SIS process displayed included the last known location of WSB-7 and that the node had not been removed from the SIS database. The error in reporting may again be attributed to a software problem with SIS.

At the conclusion of the Phase IV test several interesting results were identified:

1. Sufficient links between nodes were formed to create a stable wireless network.
2. The detection data, although captured by the PIR sensor, was not forwarded to the base station; this may be attributed to the high frequency of detections produced as a result of the turbulent water surface and may flag the need to modify the SIS protocol to allow for a more explicit means of determining duplicate reports, such as a report identifier.
3. Accurately emplacing the WSBs was difficult in the ocean due to the drift of the buoys after the anchor had been released, an uneven ocean floor, and the ability to maneuver the deployment vessel on the constantly water surface.
4. Wireless links were formed utilizing the 900 MHz radios at ranges up to 250 meters.
5. Records were not maintained and updated by the SIS database.

6. The foam ballast may slip over a period of time and a solution such as a wooden dowel can be utilized to prevent the slip.

6. Future Testing

Several areas for further or additional exploration should be considered. Some such areas include:

- The addition of WSBs to create a larger WSN, or alternate topologies implemented to observe network behavior. Topologies that include the perimeter concept or a multi-layered perimeter would enhance the feasibility of providing security for naval vessels and seabases.

- The WSBs were difficult to accurately emplace, therefore additional deployment methods and techniques should be investigated, although real world implementations may not be as constrained by the emplacement accuracy so long as the nodes are accurately reporting there location upon network activation.

  Placing sticker tape or a similar obstruction over the PIR sensors or simply turning them off may improve the overall quality of the wireless network by reducing extraneous data content. Testing the network without the PIR sensors may determine the cause of reporting delays.

- Modalities not as sensitive as the PIR sensors may provide a suitable sensing capability for the WSBs; alternate sensors should be investigated and tested. Several existing devices to include LiDAR, passive sonar, cameras, and laser range finders would provide interesting results.

  A more stable mount on the buoys to support the node may prove desirable depending on the sensor utilized; a gimbal mount may be of interest.

- Alternate networking protocols, such as Long Term Evolution (LTE) or Cosmic Hot Interstellar Plasma Spectrometer satellite (CHIPSat) based radio devices should be investigated to enhance the ranges for communication, which is vital if substantial stand-off is required to offer protection.

  Power is often a significant concern, therefore alternate or clean power sources such as wind or solar may be a valid direction for future testing.

- Alternate types of nodes such as the ARGUS perimeter system may be interesting to test and compare to the ADAPT nodes.

- Although not implemented in this thesis, the MSAT is a valuable tool that would enhance the situational awareness of the network and of any intrusions.
- Testing various scenarios of intrusions such as a direct, multi-directional, or diversionary attack would further validate the concept being presented.
- Verify the operation of the SIS protocol to determine whether it is responsible for failed detection reporting by the PIR sensors or incorrect location reporting to the base station.

F. CHAPTER SUMMARY

This chapter reported that the spar-buoy design as implemented, with the ADAPT sensor nodes attached, functioned as intended. The tests revealed that a WSB constructed using COTS products was able to achieve satisfactory communication; however, the PIR sensors performed poorly, suggesting that alternate sensing devices should be implemented with the design. The SIS process that maintains the data records should also be further investigated to determine the discrepancies in reporting. In conclusion, the tests that were conducted determined that the ADAPT sensor nodes are suitable, and could be implemented in creating an ad hoc network on an open ocean environment.

THIS PAGE INTENTIONALLY LEFT BLANK

V. SUMMARY AND CONCLUSIONS

A. SUMMARY

The concept of using wireless sensor networks housed on buoys for perimeter security of naval vessels and seabases to provide early warning of an attack was investigated. The concept for the system is to mount wireless sensor nodes on buoys for the purpose of creating a wireless sensor network (WSN), and then relaying detection information through that ad hoc network to a central base station responsible for monitoring approaches to a naval vessel. The concept of perimeter security and its implementation throughout the ages, and how it can be relevant to naval security was discussed. It was identified that the current threat of a small surface vessel based suicide attack is relevant in modern times, as indicative of recent historical events. Present AT/FP doctrine suggests that additional measures should be emplaced to mitigate terrorist attacks against naval vessels. Devices such as sonar can detect sub-surface threats and unmanned vehicles may identify threats above the surface; however, additional sensors utilizing modern technology and a self-forming, as well as self-healing, network could further diminish attacks against high value U.S. vessels by providing additional advanced warning. WSNs, in the form of the unattended ground sensors (UGSs) developed by DARPA, address this with the construction of such an ad hoc network, particularly since these sensor nodes were designed to accommodate emerging sensor technology, such as light detection and ranging (LiDAR) systems. The USMC has explicitly stated the need for enhanced security during future operations in the littoral regions. WSBs address this requirement by using existing devices that leverage COTS components to increase situational awareness and enhance AT/FP perimeter security for military vessels and seabases.

The selection and design of the spar-buoy was presented as it pertained to the proper utilization of the ADAPT nodes to form the WSN. To validate the feasibility of mounting sensor nodes on buoys, a spar-buoy design was modified. The modified spar-buoys were constructed using materials acquired from local venders to produce the components.

The 802.11n WiFi and 900 MHz radio communication served as the basis for the formation of the ad hoc network. The formation of the network was described and how the nodes sense and communicate threats by transmitting their data. Upon establishment of the MANET the nodes were able to report locations, links between nodes, and tracks using the SIS process. Detection reports were suppressed by the sensor nodes: further analysis of the sensor node host operating system (SIS) and reporting protocol remains to be accomplished to determine whether the protocol can be adapted for the high incidents of detections generated by the sea-surface motion. The SIS process operating on each of the nodes incorporated a peer-to-peer database that managed the data on the nodes and allowed sharing of information between neighbors.

The system prototype tests were divided into four phases, with two conducted on land and two conducted on sea. Phase I tested the range of the WiFi 802.11n protocol that the nodes utilized to communicate with the base station. The results were disconcerting as the location and detection reports from the nodes were often delayed or not reported. It is suspected that this was due to faulty nodes, noise in the operating area, or a software concern with the SIS process. Phase II tests assessed the legitimacy of the proposed topology on a compressed scale, and to determined that the ADAPT nodes were able to successfully establish a mobile ad hoc network (MANET). The spar-buoy prototype design was successfully tested in Phase III and a discrepancy identified which required the anchor connection point to be relocated.

During Phase IV the ability to mount ADAPT wireless sensor nodes on buoys and form a WSN was confirmed. The 900 MHz radio formed wireless links at ranges up to 250 meters, which is a satisfactory range for this system. Towards the conclusion of Phase IV testing, the SIS database maintained old data records that displayed outdated buoy positions and statuses. This indicated a critical concern with the implementation of the internal node location tracking algorithm and requires further analysis, an effort beyond the scope of this thesis.

B. PERFORMANCE

Validating the concept of wireless sensor nodes mounted on buoys to provide perimeter security for naval vessels and seabases required practical testing, as noted. The performance assessment involved confirming the connectivity of the proposed network, particularly the ability of nodes to form a multi-hop ad hoc network in a typical sea-surface environment. Since the sensor nodes would be mounted on buoys, the buoys needed to support the device in a manner that would allow the network to function. The buoy proved stable and while on the water the node was able to communicate to the base station.

Testing the network of WSBs on the ocean surface, in the environment in which they would be operating, was successful. Locations and links between nodes were reported to the base station at various intervals and ranges. However, the PIR detections were not. After reviewing the logs for the sensor nodes it was determined that the PIR sensors were capturing detections; but the detections were not forwarded. Towards the end of the testing, the SIS database failed to maintain accurate records and maintained outdated information; further experiments are required to resolve forwarding the PIR sensor data. The practical testing met all the performance parameters required to validate that wireless sensor nodes mounted on buoys would establish a functional network and would contribute to providing perimeter security for naval vessels and seabases. With the success of the ocean testing, additional experiments are required involving incorporation of more complex sensor systems, alternate deployment-in-depth topologies, and scenario-based evaluations.

C. RECOMMENDATIONS FOR FUTURE WORK

The purpose of this thesis was to design and implement a prototype sea-based autonomous sensor network leveraging the advanced ADAPT sensor node. During testing numerous shortfalls were identified. In addition to the acknowledged shortfalls, other areas for further research and exploration to enhance the feasibility of the overarching concept were generated; several of these areas are described below.

1. Alternate Sensor Node Configurations

While PIR sensors are a highly useful modality for traditional UGS that are deployed on solid ground, utilizing PIR sensors, in conjunction with the SIS protocol, in an ocean environment proved to be ineffective, thus alternate modalities should be investigated and tested for use on WSBs. Several devices are available that would potentially resolve the requirement of detecting foreign objects on the ocean surface. An example of such a device is LiDAR, which could provide both a 2-D horizontal scan or 3-D scan, with a range up to 80 meters. LiDAR should be a primary consideration; however, passive sonar may also be a suitable modality that could detect objects just beneath the ocean surface. The combination of both LiDAR and passive sonar on a single buoy would be possible and may significantly enhance the effectiveness and applicability of the WSB system for perimeter security.

The purpose of the spar-buoys were to provide stability and a designated height above the surface for the ADAPT nodes to operate; however, as stable as the spar-buoys were they still experienced motion due to the oceanic effects. Although the oceanic effects did not prove detrimental to the formation of a MANET it may have contributed to the ineffectiveness of the PIR sensors. To minimize motion effects a gimbal mount could be utilized; a gimbal mount would provide horizontal stability but not vertical stability since the ocean swell would still cause the buoy to rise and sink along the vertical axis. The gimbal mount may not have an effect on the functionality of the PIR sensor, but it would be highly useful should the LiDAR be incorporated into the design.

During the conduct of the tests described in this thesis, a notable shortfall is the range of the WiFi 802.11n protocol. With a maximum range of only 250 meters, a longer ranging networking protocol is required to provide adequate standoff for the vessel against incoming surface threats. Alternatives to 802.11n to investigate would be Long Term Evolution (LTE) or Cosmic Hot Interstellar Plasma Spectrometer satellite (CHIPSat). Both of these alternatives would have a range far exceeding 250 meters and be able to adequately mitigate the standoff concern, allowing for the link to the base station to be extended to support operationally relevant stand-off distances. Inter-node

communications links, though, must consider the operational range of the sensors hosted on the WSBs.

Power consumption is always a primary concern for wireless devices. The ADAPT nodes would only function for several days while deployed on the WSBs, and fewer days if the level of activity was high, thereby forcing the sensor nodes to remain in an active duty cycle longer resulting in greater power consumption. Some modalities and networking devices may consume additional power compared to the ADAPT nodes and further reduce operating time. Some possible solutions to the power concern would be to add additional batteries to the spar-buoy design doing dual duty serving as additional ballast, or adding clean power devices that utilize wind or solar to increase the lifespan of the batteries. These suggested solutions would prolong the operating time of the WSB; however, they would add significant weight to the buoys and require additional floatation support.

Alternate wireless sensor nodes exist that would be interesting to test. The ARGUS perimeter security system by Intelligent Automation Inc. incorporates the same modalities as the ADAPT sensors. Comparing the sensor nodes would produce valuable information in regards to the capabilities, specifically the PIR sensors. The assumption that the developmental SIS process was the reason for many of the issues encountered during the tests in this thesis could be verified.

2. Future Work

The tests conducted as part of this thesis confirmed the feasibility of establishing a WSN on the ocean surface by mounting pre-existing ADAPT UGS to spar-buoys. The tests confirmed that the concept was indeed possible with respect to the networking aspect; however, substantial tests and additional modification are required before the over-arching concept of using WSBs to protect naval vessels and seabases can be validated. Future work may include the implementation of a larger WSN to test the ability of the nodes to interact on a larger scale, provide defense/detections in-depth in an ocean environment, and to identify connectivity limitations not anticipated or addressed by previous testing. Expanding the network would also allow for further creativity when

designing the most effective topology to implement; comparing topologies would provide interesting insight into potential "gaps" in the security perimeter, the behavior of the network, or the impact of stand-off distances on network performance and reporting.

During the Phase IV test, it was difficult to accurately emplace the WSBs; various deployment methods and techniques should be investigated to improve both the accuracy and efficiency of deploying the WSBs according to the desired topology. Phase IV tests not only proved that it was difficult to establish a topology but that the PIR sensors did not produce the data as desired.

Further testing of the PIR sensors" functionality on the water surface is essential. The performance of the PIR sensors and subsequent reporting by the SIS protocol should be assessed where the WSBs are on calm water surface, such as an inner-bay with unobstructed sensors field of view so as to ensure the performance of the sensor is not impaired by the water surface. The purpose would include determining the effects the PIR sensors have on the sea-borne network and to what extent extraneous data is produced. This test may determine the cause of reporting delays.

The final implementation of the WSB system includes a GUI that the human user may utilize to observe the topology, node status, and be alerted to detections that display a breach in the perimeter and vector of the approaching threat. The MSAT is a valuable tool, and although not implemented in this thesis would enhance situational awareness and assess the conditions described. Using MSAT to test various scenarios of intrusions such as a direct, multi-directional, or diversionary attack would further validate the concept being presented.

An aspect not previously mentioned is the information security of the network. Research into information security is an imperative requirement before fielding the WSB system, as is operations in an electronically jammed environment; these are necessary avenues that should be pursued. Denial of service and unauthorized access to the network or MSAT would be detrimental to the security of the vessels and seabases.

As discussed in Chapter II, similar devices in the form of unmanned vehicles exist to mitigate threats; these devices include aerial, surface, and subsurface vehicles.

Integrating the unmanned vehicles with the sensor nodes would enhance the surveillance and ultimately the force protection of the naval vessels.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. OPERATION CHECKLIST

Charge Nodes to ~4.000 volts (no light will indicate the devices are charging)

Using Setup Computer (Thinkpad)
Connect nodes to Setup computer using green plug cord
~$ adb devices (List of devices attached – not connected to network)
~$ watch adb devices (List of devices attached – connected to network)

==========

Image the nodes with ADAPT OS

With nodes connected to Setup computer using green plug cord
~$ cd ~/Working/srb-adapt- install-April-Demo_v09272014/

Full Image Installation:
$ ./install.sh -u -x

- Select 'y' for continue without root privileges
- Select 'y' to continue
- This will take several minutes, observe that GroundRadio PASSED.

SAS only Installation: //do this if only SAS protocol is required
$ ./install.sh -u -x SAS
$ getVersion.sh version //Check ensuring MD5 of SAS versions are same (i.e. 8dee7b72), and ensure Volt is approx. 4.000.

==========

Mission Preparation

Ensure in the following directory:
$ cd ~/Working/srb-adapt- install-April-Demo_v09272014/
$ ./setupSrb4demo.sh //Pushes mission.app, clears logs, shuts off WiFi

$ adball shell ifconfig wlan0 //Tells IP address of nodes, which is critical to telnet into nodes to stop after testing

Turn off nodes with red plug to allow changes to take effect

==========

Deploying Nodes

From Base Station (Dell) Computer:
Ensure in the following directory:
$ cd ~/Working
:~Working/sis -init ./sal.adapt.create.sql & //Starts SIS as a background process

Once sis is running on Base Station Computer, Start nodes with green plug

(wait at least 5 minutes for nodes to acquire GPS fix)

Start Sitmap (graphical map)
$ sitmap &

$ watch process location //Computer shows nodes connected
$ watch process detection //Computer shows node detections
$ watch process link //Computer shows node links
$ watch process track //Computer shows node tracks

==========

Retrieving Nodes

Preserve Logs:
Telnet into nodes to stop mission, which preserves logs
$ telnet <*ip address of node*> stop mission //Telnet into nodes to stop mission

If you want to preserve logs, DO NOT shut them down with red plug!
Connect nodes to computer with green USB plug
$ mkdir test20151118nps //Make directory for test
$ cd test20151118nps //change into directory and pull log files from nodes that are connected via USB hub
$ adball pull /sdcard/ //Pulls all files from node log folder

Now, insert red plug

$ Gedit journal <nid>.17 //Views journal log-file for particular nodes

==========

Tool kit

$ lsusb //Show attached usb devices
$ adb -s < node id > shell //Login to command line of node
$ adb devices //Show attached nodes
$ adball shell svc wifi enable //Turn wifi back on – adball shell will cycle through all connected devices if more than 1 is connected
$ adball reboot //Can't do after install, but can later after changing networks to get new DHCP → IP assignment
$ adball shell ifconfig wlan0 //Tells IP address of nodes, which is critical to telnet into nodes to stop after testing
$ adball shell start mission
$ adball shell stop mission
$ adball shell nid //Gets node ids
$ adball push mission.app /data/app/sas/etc/mission.app
//Push mission.app to all nodes
$ adball shell cat /data/app/sas/etc/mission.app
//View contents of mission.app for all nodes

$ adball reboot
$ killall -9 sis //Kill sis
$ md5sum file.txt
$ adb -s f5e5af2 shell

Before deploying – tip from Billy
$ getVersion.sh version
$ adball shell ls /sdcard/log
$ adball shell stop mission
$ adball shell rm /sdcard/log/*

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. PHASE IV TEST PLAN

Equipment Required:

- 8 x Spar Buoys
- 12 x ADAPT Nodes
- Green/Red Plugs
- Lenovo Thinkpad (Setup Computer)
- Dell Laptop (Base Station)
- 2.4 GHz Repeater
- Verizon MiFi Hotspot
- Dell Router
- Power strip
- Appropriate power cords
- Yeti 400 Battery
- Operations Checklist
- Test Sheet
- Camera
- GPS

Testing Plan Details:

Intent is to confirm the ranges where both radios (WiFi 802.11n and 900MHz ground radio) function correctly in forming the ADHOC wireless network.

Method:

The purpose of the Phase IV test is to confirm that the Wireless Sensor Buoys (WSBs) are able to form an ADHOC wireless network while on the ocean surface. The test will consist of aligning eight WSBs in a single file at 30 meter dispersion creating a total distance from the Base Station to the eighth WSB of 240 meters. The eighth buoy is beyond the maximum distance that a single node would be able to communicate with the Base Station; however, buoys dispersed at 30 meter increments should be able to share information from the furthest node via the intermediate nodes to the Base Station.

Upon confirming that the nodes are effectively communicating and that the ADHOC network is functioning correctly the dispersion between WSBs will be increased. Three series of dispersion distances will be tested beginning with 30 meters, then 60 meters, and finally 90 meters. If the WSBs maintain effective communication at a dispersion of 90 meters, and if time permits, then the distances will be further increased to 120 meters or until communication is no longer effective. A representation of the test series is depicted below.

Test Series 1: Confirm the range and network

```
v       *       *       *       *       *       *       *       *
B.S.    1       2       3       4       5       6       7       8
|---30---|---30---|- - -                                 ---240---|
```

Test Series 2: Remove alternate nodes to confirm node inter-connectivity and ranges

```
v       *       *       *       *       *       *       *       *
B.S.    6       4       2       8       7       5       3       1
|---60---|---60---|- - -                                 ---480---|
```

Test Series 3: Expand range further to confirm node inter-connectivity and ranges

```
v       *       *       *       *       *       *       *       *
B.S.    2       5       1       3       7       8       4       6
|---90---|---90---|- - -                                 ---810---|
```

Test Series 4: Expand range further to confirm node inter-connectivity and ranges

```
v       *       *       *       *       *       *       *       *
B.S.    3       6       4       8       7       1       5       2
|--120--|--120--|- - -                                 ---960---|
```

Sensor Test: Test functionality of the PIR sensors

```
v       *       *       *       *       *       *       *       *
B.S.    3       6       4       8       7       1       5       2
|--120--|--120--|- - -                                 ---960---|
```

Details of the test:

- Load buoys onto vessel
- Launch boat
- Attach nodes to buoys (Numbers must correspond)
- Setup Base Station
- Activate SIS
- Turn on Nodes
- Deploy buoys 8 through 1at 30-meter intervals taking note of location, and then position boat 30 meters from buoy-1
- Collect Data (Location, Link, Detection)
- **Conduct Test Scenario 1**

- Collect buoys 2,4,6,8 and disperse at 60-meter intervals buoys 8,2,4,6.
- position boat 60 meters from buoy-6
- **Conduct Test Scenario 2**

- Collect buoy-4 and move down 30 meters creating a distance of 90 meters between 6 & 4
- Collect buoy-2
- Collect buoy-7 and move down 30 meters creating a distance of 90 meters between 8 & 7
- Collect buoy-5
- Collect buoy-1 and move down 30 meters creating a distance of 90 meters between 3 & 1
- Deploy buoy-5 90 meters from buoy-1, and buoy-2 90 meters from buoy-5
- position boat 90 meters from buoy-2
- **Conduct Test Scenario 3**

- ***If Test Scenario 3 was successful, proceed to next set of ranges (120-m)**
- Collect buoy-5 and move down 30 meters creating a dist. of 120 meters between 2 & 5
- Collect buoy-1 and move down 60 meters creating a dist. of 120 meters between 5 & 1
- Collect buoy-3
- Collect buoy-8 and move down 30 meters creating a dist. of 120 meters between 7 & 8
- Collect buoy-4 and move down 60 meters creating a dist. of 120 meters between 8 & 4
- Collect buoy-6 and move down 90 meters creating a dist. of 120 meters between 4 & 6
- Deploy buoy-3 120 meters from buoy-6, and then position boat 120 meters from buoy-3.
- **Conduct Test Scenario 4 (if required)**

- **Conduct Sensor Test** (Drive boat past WSBs in a serpentine while monitoring SIS)
- Collect all buoys
- Retrieve nodes and acquire logs

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] ARA E-UGS Unattended ground sensors provide seismic early warning security. (2013, Mar. 26). Applied Research Associates, Inc. [Online]. Available: http://forcepro.ara.com/ara-e-ugs-unattended-ground-sensors-provide-seismic-early-warning-security-0

[2] R.F. Harrington, "Unattended ground sensors for Expeditionary Force 21 Intelligence Collections," M.S. thesis, Dept. Information Warfare Systems Engineering, Naval Postgraduate School, Monterey, CA, 2015. (12)

[3] L. S. Howeth, *History of Communications-Electronics in the United States Navy*, Washington, DC: U.S. Government Printing Office, 1963, pp. 471–478.

[4] B.C. Palm and R.P. Richter, "Mobile situational awareness tool: Unattended ground sensor-based remote surveillance system," M.S. thesis, Dept. Computer Science, Naval Postgraduate School, Monterey, CA, 2014. (5,17,30,31,33,45-48,50-53)

[5] Marine Corps Combat Development Command, "Expeditionary Force 21 Capstone Concept," (5,8-11,15,19,20,22,36-38,42,43)-March 2014

[6] Federal Bureau of Investigation. Reports and publications, terrorism 2000/2001. [Online]. Available: https://www.fbi.gov/stats-services/publications/terror/terrorism-2000-2001. Accessed Jun, 30, 2015.

[7] *BBC News*. "Yemen ship attack 'was terrorism.' " (2002, Oct. 13). [Online]. Available: http://news.bbc.co.uk/2/hi/middle_east/2324431.stm

[8] S. Al-Atrush. (2014, Nov. 12). " 'Terror' attack on Egypt naval vessel leaves 8 servicemen missing." *Yahoo News* [Online]. Available: http://news.yahoo.com/terror-attack-egypt-naval-vessel-leaves-8-servicemen-230421503.html

[9] Department of Defense, *DOD USS Cole Commission Report*, Executive Summary, 9 January, 2001

[10] *USS George Washington* (CVN 73) Instruction 3300.53, 31 Mar 2015, pp 1–28, 1-29,7-1,7-2,7-3.

[11] E. J. Nelson, "Passive and active sonar prosecution of diesel submarines by nuclear submarines," M.S. thesis, Dept. Operations Research, Naval Postgraduate School, Monterey, CA, 2008. (1,8,9,21)

[12] RQ-8A and MQ-8B Fire Scout unmanned aerial vehicle (UAV). (2009, Feb. 18). U.S. Navy. [Online]. Available: http://www.navy.mil/navydata/fact_display.asp?cid=1100&tid=2150&ct=1

[13] *Jane's* unmanned maritime vehicles and systems (2014, Sep. 19). IHS Aerospace, Defence & Security. [Online]. Available: https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=Reference&ItemId=+++1323676&Pubabbrev=JUMV

[14] . U.S. Navy. Seafox [Online]. Available: http://www.navy.com/about/equipment/drones.html#underwater-drones. Accessed Oct. 16, 2015.

[15] F. Zhao and L. J. Guibas, *Wireless Sensor Networks: An Information Processing Approach*, San Francisco, CA: Morgan Kaufmann, 2004, pp. xiii.

[16] 58 - - Unattended Ground Sensor (UGS) Systems. (2009, Jun. 6). Federal Business Opportunities. [Online]. Available: https://www.fbo.gov/index?&s=opportunity&mode=form&id=73352cc5901de9929995d6751fc55355&tab=core&tabmode=list

[17] C. Lawrence, *ADAPTable Sensor System (ADAPT)*. DARPA. [Online.]. Available: http://www.darpa.mil/program/adaptable-sensor-system. Accessed Oct. 19, 2015.

[18] T. Hammel and M. Rich, "ADAPT smart munitions: Summer camp final demonstration," presented at Naval Postgraduate School, Monterey, CA, Sept. 26, 2013, PowerPoint pp. 2, 7–9, 12,13,15,18,19,22,25-28.

[19] Argus (TM) Perimeter Security System. (n.d.). Intelligent Automation, Inc. [Online]. Available: http://www.i-a-i.com/?product/argus. Accessed Nov. 3, 2015.

[20] M. Kane. (2009). C.A.D./Mapping Services, Inc. Harbor Offshore, Inc. [Online]. Available: http://www.cadmappingservices.com/HARBOR2.html

[21] Equipment items: Containment systems. (2015). Global Diving & Salvage, Inc. [Online]. Available: https://www.gdiving.com/node/124

[22] Spar Buoy. (n.d.). *Wikipedia*. Available: https://en.wikipedia.org/wiki/Spar_buoy. Accessed Nov. 3, 2015.

[23] J. Joseph and C. Merriam, "Initial modified spar buoy design," unpublished.

[24] Goal Zero Yeti 400 Solar Generator. (n.d.). Goal Zero. [Online]. Available: http://www.goalzero.com/p/165/Goal-Zero-Yeti-400-Solar-Generator. Accessed Nov. 3, 2015.

[25] P. Belanger. (2007, May 31). 802.11n delivers better range. [Online]. Available: http://www.wi-fiplanet.com/tutorials/article.php/3680781

[26] K. Rajesh. (2009, Jun. 11). What is IEEE 802.11n, what are the advantages and challenges for 802.11n in Wi-Fi networks? [Online]. Available: http://www.excitingip.com/186/what-is-ieee-80211n-what-are-the-advantages-and-challenges-for-80211n-in-wi-fi-networks/

[27] A. Birk, "3D mapping in marine environments," Jacobs University, PowerPoint, pp. 9, 10.

[28] Sea Anchor. (2015, May 11). *Wikipedia*. Available: https://en.wikipedia.org/wiki/Sea_anchor. Accessed Dec. 11, 2015.

[29] 802.11n. (2012, Nov. 2012). Tech-FAQ. [Online]. Available: http://www.tech-faq.com/80211n.html.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California